



# **SnapCenter software Softwaredokumentation**

SnapCenter software

NetApp  
September 29, 2025

This PDF was generated from <https://docs.netapp.com/de-de/snapcenter-61/index.html> on September 29, 2025. Always check docs.netapp.com for the latest.

# Inhalt

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| SnapCenter software Softwaredokumentation .....                                        | 1   |
| Versionshinweise .....                                                                 | 2   |
| Versionshinweise .....                                                                 | 2   |
| Unterstützte Upgradepfade für SnapCenter .....                                         | 2   |
| Erste Schritte .....                                                                   | 3   |
| Erfahren Sie mehr über die SnapCenter software .....                                   | 3   |
| SnapCenter -Übersicht .....                                                            | 3   |
| Sicherheitsfunktionen in SnapCenter .....                                              | 7   |
| Rollenbasierte Zugriffskontrolle in SnapCenter .....                                   | 8   |
| Notfallwiederherstellung in SnapCenter .....                                           | 14  |
| Von SnapCenter benötigte Lizenzen .....                                                | 14  |
| SnapMirror Active Sync in SnapCenter .....                                             | 17  |
| Schlüsselbegriffe des Datenschutzes .....                                              | 18  |
| Von SnapCenter unterstützte Speichersysteme und Anwendungen .....                      | 20  |
| Authentifizierungsmethoden für SnapCenter -Anmeldeinformationen .....                  | 20  |
| Unterstützte SnapCenter -Vorgänge für ASA r2-Systeme .....                             | 22  |
| Schnellstart für die SnapCenter software .....                                         | 23  |
| Installieren und Konfigurieren von SnapCenter Server .....                             | 24  |
| Vorbereiten der Installation des SnapCenter -Servers .....                             | 24  |
| Voraussetzungen für die Installation von SnapCenter Server .....                       | 24  |
| Registrieren Sie sich, um auf die SnapCenter software zuzugreifen .....                | 31  |
| Multi-Faktor-Authentifizierung (MFA) .....                                             | 32  |
| Installieren des SnapCenter -Servers .....                                             | 42  |
| Installieren Sie den SnapCenter -Server auf einem Windows-Host .....                   | 42  |
| Installieren Sie den SnapCenter -Server auf einem Linux-Host .....                     | 46  |
| SnapCenter registrieren .....                                                          | 50  |
| Melden Sie sich mit der RBAC-Autorisierung bei SnapCenter an .....                     | 50  |
| Konfigurieren des SnapCenter -Servers .....                                            | 54  |
| Hinzufügen und Bereitstellen des Speichersystems .....                                 | 54  |
| Hinzufügen von Controller-basierten Lizenzen für SnapCenter Standard .....             | 77  |
| Konfigurieren der Hochverfügbarkeit .....                                              | 82  |
| Konfigurieren der rollenbasierten Zugriffssteuerung (RBAC) .....                       | 86  |
| Konfigurieren der Überwachungsprotokolleinstellungen .....                             | 115 |
| Konfigurieren Sie sichere MySQL-Verbindungen mit SnapCenter Server .....               | 117 |
| Konfigurieren der zertifikatsbasierten Authentifizierung .....                         | 123 |
| Zertifikatbasierte Authentifizierung aktivieren .....                                  | 123 |
| Exportieren Sie Zertifikate der Zertifizierungsstelle (CA) vom SnapCenter Server ..... | 123 |
| Importieren Sie das CA-Zertifikat in die Windows-Plug-In-Hosts .....                   | 124 |
| Importieren Sie das CA-Zertifikat in die UNIX-Plug-in-Hosts .....                      | 125 |
| Exportieren von SnapCenter -Zertifikaten .....                                         | 126 |
| Konfigurieren des CA-Zertifikats für den Windows-Host .....                            | 127 |
| CA-Zertifikat-CSR-Datei generieren .....                                               | 127 |
| CA-Zertifikate importieren .....                                                       | 128 |

|                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------|-----|
| Abrufen des CA-Zertifikatfingerabdrucks . . . . .                                                                      | 129 |
| Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten . . . . .                                    | 129 |
| Konfigurieren des CA-Zertifikats mit der SnapCenter -Site . . . . .                                                    | 130 |
| Aktivieren von CA-Zertifikaten für SnapCenter . . . . .                                                                | 131 |
| Konfigurieren des CA-Zertifikats für den Linux-Host . . . . .                                                          | 131 |
| Konfigurieren Sie das Nginx-Zertifikat . . . . .                                                                       | 131 |
| Konfigurieren des Überwachungsprotokollzertifikats . . . . .                                                           | 132 |
| Konfigurieren des SnapCenter -Dienstzertifikats . . . . .                                                              | 132 |
| Konfigurieren und Aktivieren der bidirektionalen SSL-Kommunikation auf dem Windows-Host . . . . .                      | 132 |
| Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host . . . . .                                  | 133 |
| Aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host . . . . .                                     | 135 |
| Konfigurieren und Aktivieren der bidirektionalen SSL-Kommunikation auf dem Linux-Host . . . . .                        | 137 |
| Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host . . . . .                                    | 137 |
| Aktivieren Sie die SSL-Kommunikation auf dem Linux-Host . . . . .                                                      | 138 |
| Konfigurieren von Active Directory, LDAP und LDAPS . . . . .                                                           | 139 |
| Registrieren nicht vertrauenswürdiger Active Directory-Domänen . . . . .                                               | 139 |
| Konfigurieren Sie IIS-Anwendungspools, um Active Directory-Leseberechtigungen zu aktivieren. . . . .                   | 141 |
| Konfigurieren des CA-Client-Zertifikats für LDAPS . . . . .                                                            | 141 |
| Schützen Sie Microsoft SQL Server-Datenbanken . . . . .                                                                | 143 |
| SnapCenter -Plug-in für Microsoft SQL Server . . . . .                                                                 | 143 |
| Übersicht über das SnapCenter -Plug-in für Microsoft SQL Server . . . . .                                              | 143 |
| Was Sie mit dem SnapCenter Plug-in für Microsoft SQL Server tun können . . . . .                                       | 143 |
| SnapCenter Plug-in für Microsoft SQL Server-Funktionen . . . . .                                                       | 144 |
| Unterstützung für asymmetrische LUN-Zuordnung in Windows-Clustern . . . . .                                            | 145 |
| Vom SnapCenter Plug-in für Microsoft SQL Server unterstützte Speichertypen . . . . .                                   | 146 |
| Empfehlungen zum Speicherlayout für das SnapCenter -Plug-in für Microsoft SQL Server . . . . .                         | 149 |
| Für das SQL-Plug-In sind mindestens ONTAP Berechtigungen erforderlich. . . . .                                         | 151 |
| Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für das Plug-in für SQL Server vor. . . . . | 153 |
| Sicherungsstrategie für SQL Server-Ressourcen . . . . .                                                                | 154 |
| Wiederherstellungsstrategie für SQL Server . . . . .                                                                   | 159 |
| Definieren einer Klonstrategie für SQL Server . . . . .                                                                | 162 |
| Vorbereiten der Installation des SnapCenter Plug-Ins für Microsoft SQL Server . . . . .                                | 163 |
| Installationsworkflow für das SnapCenter -Plug-in für Microsoft SQL Server . . . . .                                   | 163 |
| Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-Ins für Microsoft SQL Server . . . . .  | 164 |
| Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows . . . . .                                | 165 |
| Einrichten der Anmeldeinformationen für das SnapCenter Plug-Ins-Paket für Windows . . . . .                            | 166 |
| Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource . . . . .                                | 168 |
| Konfigurieren von gMSA unter Windows Server 2016 oder höher . . . . .                                                  | 170 |
| Installieren Sie das SnapCenter -Plug-in für Microsoft SQL Server . . . . .                                            | 171 |
| CA-Zertifikat konfigurieren . . . . .                                                                                  | 178 |
| Konfigurieren der Notfallwiederherstellung . . . . .                                                                   | 181 |
| Installieren Sie das SnapCenter Plug-in for VMware vSphere . . . . .                                                   | 183 |
| CA-Zertifikat bereitstellen . . . . .                                                                                  | 184 |

|                                                                                                                                           |     |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Konfigurieren der CRL-Datei . . . . .                                                                                                     | 184 |
| Bereiten Sie sich auf den Datenschutz vor . . . . .                                                                                       | 184 |
| Voraussetzungen für die Verwendung des SnapCenter -Plug-ins für Microsoft SQL Server . . . . .                                            | 184 |
| So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SQL Server verwendet. . . . .                                      | 185 |
| Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe . . . . .                                                       | 186 |
| Sicherungsworkflow . . . . .                                                                                                              | 186 |
| Ermitteln, ob Ressourcen für die Sicherung verfügbar sind. . . . .                                                                        | 187 |
| Migrieren Sie Ressourcen zum NetApp Speichersystem . . . . .                                                                              | 189 |
| Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken . . . . .                                                                  | 191 |
| Erstellen von Ressourcengruppen und Anfügen von Richtlinien für SQL Server . . . . .                                                      | 197 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Microsoft SQL Server-Ressourcen auf ASA r2-Systemen. . . . . | 201 |
| Voraussetzungen für die Sicherung von SQL-Ressourcen . . . . .                                                                            | 203 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets . . . . .                           | 204 |
| Sichern von SQL-Ressourcen . . . . .                                                                                                      | 205 |
| Sichern von SQL Server-Ressourcengruppen. . . . .                                                                                         | 210 |
| Überwachen Sie Sicherungsvorgänge für SQL-Ressourcen auf der Seite „SnapCenter -Aufträge“. . . . .                                        | 211 |
| Abbrechen des SnapCenter -Plug-ins für Microsoft SQL Server-Sicherungsvorgänge. . . . .                                                   | 212 |
| Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“. . . . .                                                        | 213 |
| Bereinigen der Anzahl sekundärer Sicherungen mithilfe von PowerShell-Cmdlets. . . . .                                                     | 215 |
| Wiederherstellen von SQL Server-Ressourcen . . . . .                                                                                      | 216 |
| Wiederherstellungs-Workflow . . . . .                                                                                                     | 216 |
| Voraussetzungen für die Wiederherstellung einer Datenbank. . . . .                                                                        | 216 |
| Wiederherstellen von SQL Server-Datenbanksicherungen . . . . .                                                                            | 218 |
| Wiederherstellen einer SQL Server-Datenbank aus dem sekundären Speicher. . . . .                                                          | 225 |
| Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets . . . . .                                                                 | 226 |
| Reseed Availability Group-Datenbanken . . . . .                                                                                           | 229 |
| Überwachen von Wiederherstellungsvorgängen für SQL-Ressourcen . . . . .                                                                   | 230 |
| Abbrechen von Wiederherstellungsvorgängen für SQL-Ressourcen . . . . .                                                                    | 231 |
| Klonen von SQL Server-Datenbankressourcen . . . . .                                                                                       | 232 |
| Klon-Workflow . . . . .                                                                                                                   | 232 |
| Klonen aus einer SQL Server-Datenbanksicherung . . . . .                                                                                  | 232 |
| Klon-Lebenszyklus durchführen. . . . .                                                                                                    | 240 |
| Überwachen von SQL-Datenbankklonvorgängen . . . . .                                                                                       | 243 |
| Abbrechen von SQL-Ressourcenklonvorgängen. . . . .                                                                                        | 244 |
| Einen Klon teilen . . . . .                                                                                                               | 244 |
| Schützen Sie SAP HANA-Datenbanken . . . . .                                                                                               | 246 |
| SnapCenter Plug-in für SAP HANA-Datenbanken. . . . .                                                                                      | 246 |
| Übersicht über das SnapCenter -Plug-in für die SAP HANA-Datenbank . . . . .                                                               | 246 |
| Was Sie mit dem SnapCenter Plug-in für die SAP HANA-Datenbank tun können . . . . .                                                        | 246 |
| SnapCenter Plug-in für SAP HANA-Datenbankfunktionen . . . . .                                                                             | 246 |
| Vom SnapCenter Plug-in für die SAP HANA-Datenbank unterstützte Speichertypen. . . . .                                                     | 247 |
| Für das SAP HANA-Plug-In sind mindestens ONTAP Berechtigungen erforderlich . . . . .                                                      | 248 |
| Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für SAP HANA-                                              |     |

|                                                                                                                                            |     |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Datenbanken .....                                                                                                                          | 251 |
| Backup-Strategie für SAP HANA-Datenbanken .....                                                                                            | 251 |
| Wiederherstellungsstrategie für SAP HANA-Datenbanken .....                                                                                 | 255 |
| Vorbereiten der Installation des SnapCenter Plug-ins für die SAP HANA-Datenbank .....                                                      | 257 |
| Installationsworkflow des SnapCenter Plug-ins für die SAP HANA-Datenbank .....                                                             | 257 |
| Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter -Plug-ins für die<br>SAP HANA-Datenbank .....             | 258 |
| Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows .....                                                        | 261 |
| Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux .....                                                      | 262 |
| Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für die SAP HANA-Datenbank ....                                            | 263 |
| Konfigurieren von gMSA unter Windows Server 2016 oder höher .....                                                                          | 266 |
| Installieren Sie das SnapCenter -Plug-in für SAP HANA-Datenbanken .....                                                                    | 267 |
| CA-Zertifikat konfigurieren .....                                                                                                          | 273 |
| Installieren Sie das SnapCenter Plug-in for VMware vSphere .....                                                                           | 281 |
| CA-Zertifikat bereitstellen .....                                                                                                          | 281 |
| Konfigurieren der CRL-Datei .....                                                                                                          | 282 |
| Bereiten Sie sich auf den Datenschutz vor .....                                                                                            | 282 |
| Voraussetzungen für die Verwendung des SnapCenter Plug-ins für SAP HANA-Datenbank .....                                                    | 282 |
| So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SAP HANA-<br>Datenbanken verwendet .....                            | 282 |
| Sichern von SAP HANA-Ressourcen .....                                                                                                      | 283 |
| Sichern von SAP HANA-Ressourcen .....                                                                                                      | 283 |
| Konfigurieren Sie den HDB User Store Key und den HDBSQL OS User für die SAP HANA-Datenbank                                                 | 284 |
| Ermitteln Sie Ressourcen und bereiten Sie Multitenant-Datenbankcontainer für den Datenschutz vor .                                         | 285 |
| Ressourcen manuell zum Plug-In-Host hinzufügen .....                                                                                       | 288 |
| Erstellen von Sicherungsrichtlinien für SAP HANA-Datenbanken .....                                                                         | 289 |
| Erstellen von Ressourcengruppen und Anfügen von Richtlinien .....                                                                          | 296 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für SAP HANA-<br>Ressourcen auf ASA R2-Systemen. ....             | 300 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-<br>Cmdlets für die SAP HANA-Datenbank ..... | 303 |
| Sichern Sie SAP HANA-Datenbanken .....                                                                                                     | 305 |
| Sichern von Ressourcengruppen .....                                                                                                        | 312 |
| Überwachen Sie Sicherungsvorgänge für SAP HANA-Datenbanken .....                                                                           | 312 |
| Abbrechen von Sicherungsvorgängen für SAP HANA .....                                                                                       | 314 |
| Anzeigen von SAP HANA-Datenbanksicherungen und -klonen auf der Seite „Topologie“ .....                                                     | 314 |
| Wiederherstellen von SAP HANA-Datenbanken .....                                                                                            | 316 |
| Wiederherstellungs-Workflow .....                                                                                                          | 316 |
| Wiederherstellen und Wiederherstellen einer manuell hinzugefügten Ressourcensicherung .....                                                | 317 |
| Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung .....                                                 | 321 |
| Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets .....                                                                      | 326 |
| Überwachen von Wiederherstellungsvorgängen für SAP HANA-Datenbanken .....                                                                  | 328 |
| Klonen von SAP HANA-Ressourcensicherungen .....                                                                                            | 329 |
| Klon-Workflow .....                                                                                                                        | 329 |
| Klonen einer SAP HANA-Datenbanksicherung .....                                                                                             | 330 |

|                                                                                                                              |     |
|------------------------------------------------------------------------------------------------------------------------------|-----|
| Überwachen von SAP HANA-Datenbankklonvorgängen . . . . .                                                                     | 334 |
| Einen Klon teilen . . . . .                                                                                                  | 335 |
| Löschen oder Aufteilen von SAP HANA-Datenbankklonen nach dem Upgrade von SnapCenter . . . . .                                | 336 |
| Schützen Sie Oracle-Datenbanken . . . . .                                                                                    | 338 |
| Übersicht über das SnapCenter -Plug-in für Oracle-Datenbanken . . . . .                                                      | 338 |
| Was können Sie mit dem Plug-in für Oracle Database tun? . . . . .                                                            | 338 |
| Funktionen des Plug-ins für Oracle-Datenbanken . . . . .                                                                     | 338 |
| Vom Plug-in für Oracle-Datenbank unterstützte Speichertypen . . . . .                                                        | 340 |
| Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für Plug-in für Oracle vor                        | 342 |
| Für das Plug-in für Oracle sind mindestens ONTAP -Berechtigungen erforderlich . . . . .                                      | 343 |
| Installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank . . . . .                                                   | 345 |
| Installationsworkflow des SnapCenter Plug-ins für Oracle-Datenbanken . . . . .                                               | 345 |
| Voraussetzungen für das Hinzufügen von Hosts und die Installation des Plug-In-Pakets für Linux oder AIX . . . . .            | 345 |
| Fügen Sie Hosts hinzu und installieren Sie das Plug-In-Paket für Linux oder AIX über die GUI . . . . .                       | 355 |
| Alternative Möglichkeiten zur Installation des Plug-In-Pakets für Linux oder AIX . . . . .                                   | 359 |
| Konfigurieren des SnapCenter Plug-in Loader -Dienstes . . . . .                                                              | 362 |
| Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Dienst auf dem Linux-Host . . . . .              | 365 |
| CA-Zertifikate für Plug-Ins aktivieren . . . . .                                                                             | 368 |
| Importieren Sie Daten aus SnapManager für Oracle und SnapManager für SAP in SnapCenter . . . . .                             | 369 |
| Installieren Sie das SnapCenter Plug-in for VMware vSphere . . . . .                                                         | 375 |
| CA-Zertifikat bereitstellen . . . . .                                                                                        | 375 |
| Konfigurieren der CRL-Datei . . . . .                                                                                        | 375 |
| Vorbereiten des Schutzes von Oracle-Datenbanken . . . . .                                                                    | 375 |
| Sichern Sie Oracle-Datenbanken . . . . .                                                                                     | 377 |
| Übersicht über das Backup-Verfahren . . . . .                                                                                | 377 |
| Informationen zur Sicherungskonfiguration . . . . .                                                                          | 378 |
| Voraussetzungen für die Sicherung einer Oracle-Datenbank . . . . .                                                           | 390 |
| Entdecken Sie für die Sicherung verfügbare Oracle-Datenbanken . . . . .                                                      | 391 |
| Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken . . . . .                                                         | 393 |
| Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Oracle-Datenbanken hinzu . . . . .                             | 400 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Oracle-Ressourcen auf ASA R2-Systemen . . . . . | 402 |
| Sichern von Oracle-Ressourcen . . . . .                                                                                      | 405 |
| Sichern von Oracle-Datenbankressourcengruppen . . . . .                                                                      | 408 |
| Überwachen der Oracle-Datenbanksicherung . . . . .                                                                           | 409 |
| Andere Sicherungsvorgänge . . . . .                                                                                          | 410 |
| Mounten und Unmounten von Datenbanksicherungen . . . . .                                                                     | 415 |
| Mounten einer Datenbanksicherung . . . . .                                                                                   | 415 |
| Unmounten einer Datenbanksicherung . . . . .                                                                                 | 416 |
| Wiederherstellen und Wiederherstellen von Oracle-Datenbanken . . . . .                                                       | 417 |
| Wiederherstellungs-Workflow . . . . .                                                                                        | 417 |
| Definieren Sie eine Wiederherstellungsstrategie für Oracle-Datenbanken . . . . .                                             | 417 |
| Vordefinierte Umgebungsvariablen zum Wiederherstellen bestimmter Prescript- und Postscript-                                  |     |

|                                                                                                                               |     |
|-------------------------------------------------------------------------------------------------------------------------------|-----|
| Dateien .....                                                                                                                 | 422 |
| Voraussetzungen für die Wiederherstellung einer Oracle-Datenbank .....                                                        | 424 |
| Wiederherstellen und Wiederherstellen der Oracle-Datenbank .....                                                              | 425 |
| Wiederherstellen und Wiederherstellen von Tablespace mithilfe der Point-in-Time-Wiederherstellung .....                       | 430 |
| Wiederherstellen und Wiederherstellen einer steckbaren Datenbank mithilfe der Point-in-Time-Wiederherstellung .....           | 432 |
| Wiederherstellen und Wiederherstellen von Oracle-Datenbanken mit UNIX-Befehlen .....                                          | 435 |
| Überwachen von Wiederherstellungsvorgängen für Oracle-Datenbanken .....                                                       | 435 |
| Abbrechen von Oracle-Datenbankwiederherstellungsvorgängen .....                                                               | 436 |
| Oracle-Datenbank klonen .....                                                                                                 | 437 |
| Klon-Workflow .....                                                                                                           | 437 |
| Definieren Sie eine Klonstrategie für Oracle-Datenbanken .....                                                                | 438 |
| Vordefinierte Umgebungsvariablen für klonspezifisches Prescript und Postscript .....                                          | 439 |
| Voraussetzungen für das Klonen einer Oracle-Datenbank .....                                                                   | 440 |
| Klonen einer Oracle-Datenbanksicherung .....                                                                                  | 442 |
| Klonen einer steckbaren Datenbank .....                                                                                       | 452 |
| Klonen Sie Oracle-Datenbanksicherungen mit UNIX-Befehlen .....                                                                | 457 |
| Aufteilen eines Oracle-Datenbankklons .....                                                                                   | 458 |
| Geteilter Klon einer steckbaren Datenbank .....                                                                               | 459 |
| Überwachen von Oracle-Datenbankklonvorgängen .....                                                                            | 459 |
| Aktualisieren eines Klons .....                                                                                               | 460 |
| Klon einer Pluggable-Datenbank löschen .....                                                                                  | 461 |
| Verwalten von Anwendungsvolumen .....                                                                                         | 462 |
| Was sind Anwendungsvolumina .....                                                                                             | 462 |
| Anwendungsvolumen hinzufügen .....                                                                                            | 462 |
| Backup-Anwendungsvolumen .....                                                                                                | 463 |
| Klonen Sie die Datenträgersicherung der Anwendung .....                                                                       | 466 |
| Schützen Sie Windows-Dateisysteme .....                                                                                       | 468 |
| SnapCenter Plug-in für Microsoft Windows-Konzepte .....                                                                       | 468 |
| Übersicht über das SnapCenter -Plug-in für Microsoft Windows .....                                                            | 468 |
| Was Sie mit dem SnapCenter Plug-in für Microsoft Windows tun können .....                                                     | 468 |
| Funktionen des SnapCenter -Plug-ins für Windows .....                                                                         | 469 |
| So sichert SnapCenter Windows-Dateisysteme .....                                                                              | 470 |
| Vom SnapCenter Plug-in für Microsoft Windows unterstützte Speichertypen .....                                                 | 470 |
| Für das Windows-Plug-In sind mindestens ONTAP -Berechtigungen erforderlich .....                                              | 473 |
| Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation .....                                          | 475 |
| Definieren Sie eine Sicherheitsstrategie für Windows-Dateisysteme .....                                                       | 476 |
| Quellen und Ziele von Klonen für Windows-Dateisysteme .....                                                                   | 478 |
| Installieren Sie das SnapCenter -Plug-in für Microsoft Windows .....                                                          | 478 |
| Installationsablauf des SnapCenter Plug-ins für Microsoft Windows .....                                                       | 478 |
| Installationsanforderungen für das SnapCenter -Plug-in für Microsoft Windows .....                                            | 479 |
| Hosts hinzufügen und SnapCenter Plug-in für Microsoft Windows installieren .....                                              | 483 |
| Installieren Sie das SnapCenter -Plug-in für Microsoft Windows mithilfe von PowerShell-Cmdlets auf mehreren Remotehosts ..... | 487 |
| Installieren Sie das SnapCenter -Plug-in für Microsoft Windows im Hintergrund über die Befehlszeile .....                     | 487 |

|                                                                                                                       |     |
|-----------------------------------------------------------------------------------------------------------------------|-----|
| Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets                                                     | 489 |
| Konfigurieren des CA-Zertifikats                                                                                      | 490 |
| Installieren Sie das SnapCenter Plug-in for VMware vSphere                                                            | 493 |
| CA-Zertifikat bereitstellen                                                                                           | 493 |
| Konfigurieren der CRL-Datei                                                                                           | 493 |
| Sichern Sie Windows-Dateisysteme                                                                                      | 494 |
| Sichern Sie Windows-Dateisysteme                                                                                      | 494 |
| Ermitteln der Ressourcenverfügbarkeit für Windows-Dateisysteme                                                        | 495 |
| Erstellen von Sicherungsrichtlinien für Windows-Dateisysteme                                                          | 496 |
| Erstellen von Ressourcengruppen für Windows-Dateisysteme                                                              | 500 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Windows-Dateisysteme auf ASA R2-Systemen | 502 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets                 | 505 |
| Sichern Sie bei Bedarf eine einzelne Ressource für Windows-Dateisysteme                                               | 506 |
| Sichern von Ressourcengruppen für Windows-Dateisysteme                                                                | 510 |
| Überwachen von Sicherungsvorgängen                                                                                    | 511 |
| Abbrechen von Sicherungsvorgängen                                                                                     | 513 |
| Anzeigen zugehöriger Sicherungen und Klone auf der Seite „Topologie“                                                  | 513 |
| Bereinigen der Anzahl sekundärer Sicherungen mithilfe von PowerShell-Cmdlets                                          | 516 |
| Wiederherstellen von Windows-Dateisystemen                                                                            | 516 |
| Wiederherstellen von Windows-Dateisystemsicherungen                                                                   | 516 |
| Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets                                                       | 521 |
| Überwachen von Wiederherstellungsvorgängen                                                                            | 524 |
| Abbrechen von Wiederherstellungsvorgängen                                                                             | 525 |
| Klonen Sie Windows-Dateisysteme                                                                                       | 526 |
| Klonen aus einer Windows-Dateisystemsicherung                                                                         | 526 |
| Überwachen von Klonvorgängen                                                                                          | 532 |
| Abbrechen von Klonvorgängen                                                                                           | 533 |
| Einen Klon teilen                                                                                                     | 534 |
| Schützen Sie Microsoft Exchange Server-Datenbanken                                                                    | 536 |
| SnapCenter Plug-in für Microsoft Exchange Server-Konzepte                                                             | 536 |
| Übersicht über das SnapCenter -Plug-in für Microsoft Exchange Server                                                  | 536 |
| Was Sie mit dem SnapCenter Plug-in für Microsoft Exchange Server tun können                                           | 537 |
| Vom SnapCenter Plug-in für Microsoft Windows und Microsoft Exchange Server unterstützte Speichertypen                 | 537 |
| Für das Exchange-Plug-In sind mindestens ONTAP Berechtigungen erforderlich                                            | 538 |
| Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation                                        | 541 |
| Definieren Sie eine Sicherungsstrategie für Exchange Server-Ressourcen                                                | 541 |
| Definieren einer Wiederherstellungsstrategie für Exchange-Datenbanken                                                 | 544 |
| Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server                                                | 545 |
| Installationsablauf des SnapCenter Plug-ins für Microsoft Exchange Server                                             | 545 |
| Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für Microsoft Exchange Server      | 546 |
| Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für Windows                                           | 550 |



|                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------|-----|
| Konfigurieren von gMSA unter Windows Server 2016 oder höher                                                               | 551 |
| Hosts hinzufügen und Plug-in für Exchange installieren                                                                    | 553 |
| Installieren Sie das Plug-in für Exchange vom SnapCenter Server-Host mithilfe von PowerShell-Cmdlets                      | 559 |
| Installieren Sie das SnapCenter -Plug-in für Exchange im Hintergrund über die Befehlszeile                                | 560 |
| Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets                                                         | 561 |
| CA-Zertifikat konfigurieren                                                                                               | 562 |
| Konfigurieren Sie SnapManager 7.x für die Koexistenz von Exchange und SnapCenter                                          | 565 |
| Installieren Sie das SnapCenter Plug-in for VMware vSphere                                                                | 567 |
| CA-Zertifikat bereitstellen                                                                                               | 567 |
| Konfigurieren der CRL-Datei                                                                                               | 567 |
| Bereiten Sie sich auf den Datenschutz vor                                                                                 | 568 |
| Voraussetzungen für die Verwendung des SnapCenter Plug-Ins für Microsoft Exchange Server                                  | 568 |
| So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von Exchange Server verwendet                          | 569 |
| Sichern von Exchange-Ressourcen                                                                                           | 570 |
| Sicherungsworkflow                                                                                                        | 570 |
| Exchange-Datenbank und Backup-Verifizierung                                                                               | 571 |
| Ermitteln, ob Exchange-Ressourcen für die Sicherung verfügbar sind                                                        | 571 |
| Erstellen von Sicherungsrichtlinien für Exchange Server-Datenbanken                                                       | 573 |
| Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Exchange-Server hinzu                                       | 581 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für Exchange Server | 584 |
| Sichern Sie Exchange-Datenbanken                                                                                          | 585 |
| Sichern von Exchange-Ressourcengruppen                                                                                    | 591 |
| Überwachen von Sicherungsvorgängen                                                                                        | 592 |
| Abbrechen von Sicherungsvorgängen für die Exchange-Datenbank                                                              | 593 |
| Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“                                                               | 594 |
| Wiederherstellen von Exchange-Ressourcen                                                                                  | 596 |
| Wiederherstellungs-Workflow                                                                                               | 596 |
| Voraussetzungen für die Wiederherstellung einer Exchange-Datenbank                                                        | 596 |
| Wiederherstellen von Exchange-Datenbanken                                                                                 | 597 |
| Granulare Wiederherstellung von E-Mails und Postfächern                                                                   | 602 |
| Wiederherstellen einer Exchange Server-Datenbank aus einem sekundären Speicher                                            | 602 |
| Reseed einer passiven Exchange-Knotenreplik                                                                               | 603 |
| Führen Sie mithilfe von PowerShell-Cmdlets für die Exchange-Datenbank ein erneutes Seeding eines Replikats durch          | 604 |
| Überwachen von Wiederherstellungsvorgängen                                                                                | 605 |
| Abbrechen von Wiederherstellungsvorgängen für die Exchange-Datenbank                                                      | 605 |
| Schützen Sie IBM Db2                                                                                                      | 607 |
| SnapCenter Plug-in für IBM Db2                                                                                            | 607 |
| Übersicht über das SnapCenter -Plug-in für IBM Db2                                                                        | 607 |
| Was Sie mit dem SnapCenter Plug-in für IBM Db2 tun können                                                                 | 607 |
| SnapCenter Plug-in für IBM Db2-Funktionen                                                                                 | 608 |
| Vom SnapCenter Plug-in für IBM Db2 unterstützte Speichertypen                                                             | 608 |

|                                                                                                                                  |     |
|----------------------------------------------------------------------------------------------------------------------------------|-----|
| Für das IBM Db2-Plug-In erforderliche Mindest ONTAP Berechtigungen . . . . .                                                     | 609 |
| Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für IBM Db2. . . . .                              | 612 |
| Backup-Strategie für IBM Db2 . . . . .                                                                                           | 612 |
| Wiederherstellungs- und Recovery-Strategie für IBM Db2 . . . . .                                                                 | 615 |
| Vorbereiten der Installation des SnapCenter -Plug-ins für IBM Db2 . . . . .                                                      | 616 |
| Installationsworkflow des SnapCenter Plug-ins für IBM Db2. . . . .                                                               | 616 |
| Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows,<br>Linux oder AIX . . . . .   | 617 |
| Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows . . . . .                                          | 622 |
| Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux. . . . .                                         | 623 |
| Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für IBM Db2 . . . . .                                            | 624 |
| Konfigurieren von gMSA unter Windows Server 2016 oder höher . . . . .                                                            | 627 |
| Installieren Sie das SnapCenter -Plug-in für IBM Db2. . . . .                                                                    | 628 |
| CA-Zertifikat konfigurieren . . . . .                                                                                            | 634 |
| Bereiten Sie sich auf den Datenschutz vor . . . . .                                                                              | 642 |
| Voraussetzungen für die Verwendung des SnapCenter Plug-Ins für IBM Db2 . . . . .                                                 | 643 |
| So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von IBM Db2 verwendet . . . . .                               | 643 |
| Sichern von IBM Db2-Ressourcen. . . . .                                                                                          | 644 |
| Sichern von IBM Db2-Ressourcen. . . . .                                                                                          | 644 |
| Automatisches Erkennen der Datenbanken . . . . .                                                                                 | 646 |
| Ressourcen manuell zum Plug-In-Host hinzufügen. . . . .                                                                          | 646 |
| Erstellen von Sicherungsrichtlinien für IBM Db2 . . . . .                                                                        | 648 |
| Erstellen von Ressourcengruppen und Anfügen von Richtlinien . . . . .                                                            | 650 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für IBM Db2-<br>Ressourcen auf ASA r2-Systemen. . . . . | 654 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-<br>Cmdlets für IBM Db2 . . . . .  | 657 |
| Sichern von Db2-Datenbanken . . . . .                                                                                            | 658 |
| Sichern von Ressourcengruppen. . . . .                                                                                           | 665 |
| Überwachen von IBM Db2-Sicherungsvorgängen. . . . .                                                                              | 666 |
| Abbrechen von Sicherungsvorgängen für IBM Db2. . . . .                                                                           | 667 |
| Anzeigen von IBM Db2-Sicherungen und -Klonen auf der Seite „Topologie“ . . . . .                                                 | 668 |
| IBM Db2 wiederherstellen . . . . .                                                                                               | 670 |
| Wiederherstellungs-Workflow . . . . .                                                                                            | 670 |
| Wiederherstellen einer manuell hinzugefügten Ressourcensicherung . . . . .                                                       | 671 |
| Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung . . . . .                                   | 675 |
| Überwachen von IBM Db2-Wiederherstellungsvorgängen . . . . .                                                                     | 677 |
| Klonen von IBM Db2-Ressourcensicherungen . . . . .                                                                               | 678 |
| Klon-Workflow . . . . .                                                                                                          | 678 |
| Klonen einer IBM Db2-Sicherung . . . . .                                                                                         | 678 |
| Überwachen von IBM Db2-Klonvorgängen . . . . .                                                                                   | 685 |
| Einen Klon teilen . . . . .                                                                                                      | 686 |
| Löschen oder Aufteilen von IBM Db2-Datenbankklonen nach dem Upgrade von SnapCenter. . . . .                                      | 687 |
| Schützen Sie PostgreSQL . . . . .                                                                                                | 689 |
| SnapCenter Plug-in für PostgreSQL . . . . .                                                                                      | 689 |

|                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------|-----|
| Übersicht über das SnapCenter -Plug-in für PostgreSQL                                                                  | 689 |
| Was Sie mit dem SnapCenter Plug-in für PostgreSQL tun können                                                           | 689 |
| SnapCenter Plug-in für PostgreSQL-Funktionen                                                                           | 689 |
| Vom SnapCenter Plug-in für PostgreSQL unterstützte Speichertypen                                                       | 690 |
| Für das PostgreSQL-Plug-In sind mindestens ONTAP Berechtigungen erforderlich                                           | 691 |
| Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für PostgreSQL                          | 694 |
| Backup-Strategie für PostgreSQL                                                                                        | 694 |
| Wiederherstellungs- und Recovery-Strategie für PostgreSQL                                                              | 697 |
| Vorbereiten der Installation des SnapCenter Plug-ins für PostgreSQL                                                    | 698 |
| Installationsablauf des SnapCenter Plug-ins für PostgreSQL                                                             | 698 |
| Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für PostgreSQL                      | 699 |
| Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows                                          | 702 |
| Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux                                        | 703 |
| Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für PostgreSQL                                         | 704 |
| Konfigurieren von gMSA unter Windows Server 2016 oder höher                                                            | 707 |
| Installieren Sie das SnapCenter -Plug-in für PostgreSQL                                                                | 708 |
| CA-Zertifikat konfigurieren                                                                                            | 714 |
| Bereiten Sie sich auf den Datenschutz vor                                                                              | 722 |
| Voraussetzungen für die Verwendung des SnapCenter -Plug-Ins für PostgreSQL                                             | 723 |
| Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von PostgreSQL verwendet werden                           | 723 |
| Sichern von PostgreSQL-Ressourcen                                                                                      | 724 |
| Sichern von PostgreSQL-Ressourcen                                                                                      | 724 |
| Automatisches Erkennen der Cluster                                                                                     | 726 |
| Ressourcen manuell zum Plug-In-Host hinzufügen                                                                         | 726 |
| Erstellen von Sicherungsrichtlinien für PostgreSQL                                                                     | 728 |
| Erstellen von Ressourcengruppen und Anfügen von Richtlinien                                                            | 732 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für PostgreSQL-Ressourcen auf ASA r2-Systemen | 736 |
| Erstellen Sie eine Speichersystemverbindung und eine Anmeldeinformation mit PowerShell-Cmdlets für PostgreSQL          | 739 |
| Sichern Sie PostgreSQL                                                                                                 | 741 |
| Sichern von Ressourcengruppen                                                                                          | 746 |
| Überwachen von PostgreSQL-Sicherungsvorgängen                                                                          | 747 |
| Abbrechen von Sicherungsvorgängen für PostgreSQL                                                                       | 748 |
| Anzeigen von PostgreSQL-Sicherungen und -Klonen auf der Seite „Topologie“                                              | 749 |
| PostgreSQL wiederherstellen                                                                                            | 751 |
| Wiederherstellungs-Workflow                                                                                            | 751 |
| Wiederherstellen und Wiederherstellen einer manuell hinzugefügten Ressourcensicherung                                  | 751 |
| Wiederherstellen und Wiederherstellen einer automatisch erkannten Clustersicherung                                     | 756 |
| Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets                                                        | 759 |
| Überwachen von PostgreSQL-Wiederherstellungsvorgängen                                                                  | 761 |
| Klonen von PostgreSQL-Ressourcensicherungen                                                                            | 762 |
| Klon-Workflow                                                                                                          | 762 |

|                                                                                                                             |     |
|-----------------------------------------------------------------------------------------------------------------------------|-----|
| Klonen einer PostgreSQL-Sicherung . . . . .                                                                                 | 763 |
| Überwachen von PostgreSQL-Klonvorgängen . . . . .                                                                           | 766 |
| Einen Klon teilen . . . . .                                                                                                 | 767 |
| Löschen oder Aufteilen von PostgreSQL-Cluster-Klonen nach dem Upgrade von SnapCenter . . . . .                              | 768 |
| MySQL schützen . . . . .                                                                                                    | 770 |
| SnapCenter -Plug-in für MySQL . . . . .                                                                                     | 770 |
| Übersicht über das SnapCenter -Plug-in für MySQL . . . . .                                                                  | 770 |
| Was Sie mit dem SnapCenter Plug-in für MySQL tun können . . . . .                                                           | 770 |
| SnapCenter Plug-in für MySQL-Funktionen . . . . .                                                                           | 770 |
| Vom SnapCenter Plug-in für MySQL unterstützte Speichertypen . . . . .                                                       | 771 |
| Für das MySQL-Plug-In erforderliche Mindest ONTAP Berechtigungen . . . . .                                                  | 772 |
| Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für MySQL . . . . .                          | 775 |
| Backup-Strategie für MySQL . . . . .                                                                                        | 775 |
| Wiederherstellungs- und Recovery-Strategie für MySQL . . . . .                                                              | 778 |
| Vorbereiten der Installation des SnapCenter -Plug-ins für MySQL . . . . .                                                   | 779 |
| Installationsablauf des SnapCenter Plug-ins für MySQL . . . . .                                                             | 779 |
| Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für MySQL . . . . .                      | 779 |
| Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows . . . . .                                     | 783 |
| Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux . . . . .                                   | 784 |
| Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für MySQL . . . . .                                         | 785 |
| Installieren Sie das SnapCenter -Plug-in für MySQL . . . . .                                                                | 788 |
| CA-Zertifikat konfigurieren . . . . .                                                                                       | 794 |
| Bereiten Sie sich auf den Datenschutz vor . . . . .                                                                         | 802 |
| Voraussetzungen für die Verwendung des SnapCenter -Plug-ins für MySQL . . . . .                                             | 802 |
| So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von MySQL verwendet . . . . .                            | 802 |
| Sichern von MySQL-Ressourcen . . . . .                                                                                      | 803 |
| Sichern von MySQL-Ressourcen . . . . .                                                                                      | 803 |
| Automatisches Erkennen der Datenbanken . . . . .                                                                            | 805 |
| Ressourcen manuell zum Plug-In-Host hinzufügen . . . . .                                                                    | 805 |
| Erstellen von Sicherungsrichtlinien für MySQL . . . . .                                                                     | 806 |
| Erstellen von Ressourcengruppen und Anfügen von Richtlinien . . . . .                                                       | 810 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für MySQL-Ressourcen auf ASA R2-Systemen . . . . . | 814 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für MySQL . . . . .   | 817 |
| MySQL sichern . . . . .                                                                                                     | 819 |
| Sichern von Ressourcengruppen . . . . .                                                                                     | 824 |
| Überwachen von MySQL-Sicherungsvorgängen . . . . .                                                                          | 825 |
| Abbrechen von Sicherungsvorgängen für MySQL . . . . .                                                                       | 826 |
| MySQL-Backups und -Klone auf der Topologieseite anzeigen . . . . .                                                          | 827 |
| MySQL wiederherstellen . . . . .                                                                                            | 829 |
| Wiederherstellungs-Workflow . . . . .                                                                                       | 829 |
| Wiederherstellen und Wiederherstellen einer manuell hinzugefügten Ressourcensicherung . . . . .                             | 829 |
| Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung . . . . .                              | 834 |
| Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets . . . . .                                                   | 836 |

|                                                                                                                                           |     |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Überwachen von MySQL-Wiederherstellungsvorgängen .....                                                                                    | 838 |
| Klonen von MySQL-Ressourcensicherungen .....                                                                                              | 839 |
| Klon-Workflow .....                                                                                                                       | 839 |
| Klonen Sie ein MySQL-Backup .....                                                                                                         | 840 |
| Überwachen von MySQL-Klonvorgängen .....                                                                                                  | 843 |
| Einen Klon teilen .....                                                                                                                   | 844 |
| Löschen oder Aufteilen von MySQL-Datenbankklonen nach dem Upgrade von SnapCenter .....                                                    | 845 |
| Schützen Sie Anwendungen mit von NetApp unterstützten Plug-ins .....                                                                      | 847 |
| Von NetApp unterstützte Plug-Ins .....                                                                                                    | 847 |
| Übersicht der von NetApp unterstützten Plug-ins .....                                                                                     | 847 |
| Was Sie mit den von NetApp unterstützten Plug-ins tun können .....                                                                        | 847 |
| Von NetApp unterstützte Plug-In-Funktionen .....                                                                                          | 848 |
| Von NetApp unterstützte Speichertypen .....                                                                                               | 849 |
| Für das von NetApp unterstützte Plug-In sind mindestens ONTAP -Berechtigungen erforderlich .....                                          | 849 |
| Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für von NetApp unterstützte Plug-Ins vor .....                 | 852 |
| Definieren Sie eine Sicherheitsstrategie .....                                                                                            | 852 |
| Sicherungsstrategie für von NetApp unterstützte Plug-Ins .....                                                                            | 853 |
| Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte, von NetApp unterstützte Plug-in-Ressourcen unterstützt werden ..... | 854 |
| Bereiten Sie die Installation von NetApp unterstützten Plug-Ins vor .....                                                                 | 854 |
| Installationsablauf der von SnapCenter NetApp unterstützten Plug-Ins .....                                                                | 854 |
| Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows, Linux oder AIX .....                   | 855 |
| Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows .....                                                       | 859 |
| Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux und AIX .....                                             | 860 |
| Einrichten von Anmeldeinformationen für von NetApp unterstützte Plug-Ins .....                                                            | 861 |
| Konfigurieren von gMSA unter Windows Server 2016 oder höher .....                                                                         | 864 |
| Installieren Sie die von NetApp unterstützten Plug-Ins .....                                                                              | 865 |
| CA-Zertifikat konfigurieren .....                                                                                                         | 872 |
| Bereiten Sie sich auf den Datenschutz vor .....                                                                                           | 880 |
| Voraussetzungen für die Verwendung der von NetApp unterstützten Plug-Ins .....                                                            | 880 |
| So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von NetApp unterstützten Plug-In-Ressourcen verwendet .....            | 881 |
| Sichern Sie von NetApp unterstützte Plug-In-Ressourcen .....                                                                              | 881 |
| Sichern Sie von NetApp unterstützte Plug-In-Ressourcen .....                                                                              | 882 |
| Ressourcen zu NetApp unterstützten Plug-ins hinzufügen .....                                                                              | 882 |
| Erstellen Sie Richtlinien für von NetApp unterstützte Plug-In-Ressourcen .....                                                            | 887 |
| Erstellen von Ressourcengruppen und Anfügen von Richtlinien .....                                                                         | 891 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Ressourcen auf ASA R2-Systemen .....                         | 895 |
| Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets .....                               | 898 |
| Sichern Sie einzelne von NetApp unterstützte Plug-In-Ressourcen .....                                                                     | 899 |
| Sichern Sie Ressourcengruppen von NetApp unterstützten Plug-In-Ressourcen .....                                                           | 904 |

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| Überwachen Sie die Sicherungsvorgänge für NetApp unterstützte Plug-In-Ressourcen                                   | 905 |
| Abbrechen von Sicherungsvorgängen für von NetApp unterstützte Plug-Ins                                             | 906 |
| Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“    | 907 |
| Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen                                                      | 909 |
| Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen                                                      | 909 |
| Wiederherstellen einer Ressourcensicherung                                                                         | 909 |
| Überwachen Sie die Wiederherstellungsvorgänge für von NetApp unterstützte Plug-In-Ressourcen                       | 914 |
| Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen                                                      | 915 |
| Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen                                                      | 915 |
| Klonen aus einer Sicherung                                                                                         | 916 |
| Überwachen Sie von NetApp unterstützte Plug-in-Ressourcenklonvorgänge                                              | 922 |
| Schützen Sie Unix-Dateisysteme                                                                                     | 924 |
| Was Sie mit dem SnapCenter Plug-in für Unix-Dateisysteme tun können                                                | 924 |
| Unterstützte Konfigurationen                                                                                       | 924 |
| Einschränkungen                                                                                                    | 925 |
| Features                                                                                                           | 925 |
| Installieren Sie das SnapCenter Plug-in für Unix-Dateisysteme                                                      | 925 |
| Voraussetzungen für das Hinzufügen von Hosts und die Installation des Plug-In-Pakets für Linux                     | 925 |
| Fügen Sie Hosts hinzu und installieren Sie das Plug-In-Paket für Linux über die GUI                                | 927 |
| Konfigurieren des SnapCenter Plug-in Loader -Dienstes                                                              | 930 |
| Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Dienst auf dem Linux-Host              | 933 |
| CA-Zertifikate für Plug-Ins aktivieren                                                                             | 936 |
| Installieren Sie das SnapCenter Plug-in for VMware vSphere                                                         | 937 |
| CA-Zertifikat bereitstellen                                                                                        | 937 |
| Konfigurieren der CRL-Datei                                                                                        | 937 |
| Bereiten Sie sich auf den Schutz von Unix-Dateisystemen vor                                                        | 937 |
| Sichern Sie Unix-Dateisysteme                                                                                      | 938 |
| Entdecken Sie die für die Sicherung verfügbaren UNIX-Dateisysteme                                                  | 938 |
| Erstellen Sie Sicherungsrichtlinien für Unix-Dateisysteme                                                          | 938 |
| Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Unix-Dateisysteme hinzu                              | 941 |
| Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Unix-Dateisysteme auf ASA R2-Systemen | 943 |
| Sichern Sie Unix-Dateisysteme                                                                                      | 946 |
| Sichern von Ressourcengruppen von Unix-Dateisystemen                                                               | 948 |
| Überwachen Sie die Sicherung von Unix-Dateisystemen                                                                | 948 |
| Geschützte Unix-Dateisysteme auf der Seite „Topologie“ anzeigen                                                    | 949 |
| Wiederherstellen und Wiederherstellen von Unix-Dateisystemen                                                       | 952 |
| Stellen Sie Unix-Dateisysteme wieder her                                                                           | 952 |
| Überwachen Sie Wiederherstellungsvorgänge für Unix-Dateisysteme                                                    | 954 |
| Klonen Sie Unix-Dateisysteme                                                                                       | 954 |
| Klonen Sie die Sicherung des Unix-Dateisystems                                                                     | 954 |
| Einen Klon teilen                                                                                                  | 956 |
| Überwachen Sie Klonvorgänge für Unix-Dateisysteme                                                                  | 957 |

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden           | 959 |
| Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden           | 959 |
| Einschränkungen                                                                  | 959 |
| Installieren Sie SnapCenter und erstellen Sie Anmeldeinformationen               | 959 |
| Installieren von SnapCenter auf einer virtuellen Azure-Maschine                  | 959 |
| Erstellen der Azure-Anmeldeinformationen in SnapCenter                           | 961 |
| Konfigurieren des Azure-Speicherkontos                                           | 962 |
| Erstellen Sie die Anmeldeinformationen zum Hinzufügen des Plug-In-Hosts          | 962 |
| Schützen Sie SAP HANA-Datenbanken                                                | 963 |
| Hosts hinzufügen und SnapCenter Plug-In für SAP HANA-Datenbank installieren      | 963 |
| SAP HANA-Datenbank hinzufügen                                                    | 964 |
| Erstellen von Sicherungsrichtlinien für SAP HANA-Datenbanken                     | 965 |
| Erstellen von Ressourcengruppen und Anfügen von SAP HANA-Sicherungsrichtlinien   | 965 |
| Sichern von SAP HANA-Datenbanken, die auf Azure NetApp Files ausgeführt werden   | 966 |
| Sichern von SAP HANA-Ressourcengruppen                                           | 967 |
| Wiederherstellen und Wiederherstellen von SAP HANA-Datenbanken                   | 968 |
| Klonen Sie die SAP HANA-Datenbanksicherung                                       | 969 |
| Schützen Sie Microsoft SQL Server-Datenbanken                                    | 970 |
| Hosts hinzufügen und SnapCenter Plug-In für SQL Server-Datenbank installieren    | 970 |
| Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken                   | 971 |
| Erstellen von Ressourcengruppen und Anfügen von SQL-Sicherungsrichtlinien        | 972 |
| Sichern von SQL Server-Datenbanken, die auf Azure NetApp Files ausgeführt werden | 973 |
| Sichern von SQL Server-Ressourcengruppen                                         | 974 |
| Wiederherstellen und Wiederherstellen von SQL Server-Datenbanken                 | 975 |
| Klonen Sie die SQL Server-Datenbanksicherung                                     | 976 |
| Schützen Sie Oracle-Datenbanken                                                  | 978 |
| Hosts hinzufügen und SnapCenter Plug-In für Oracle-Datenbank installieren        | 978 |
| Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken                       | 979 |
| Erstellen Sie Ressourcengruppen und fügen Sie Oracle-Sicherungsrichtlinien hinzu | 979 |
| Sichern von Oracle-Datenbanken, die auf Azure NetApp Files ausgeführt werden     | 981 |
| Sichern von Oracle-Ressourcengruppen                                             | 981 |
| Wiederherstellen und Wiederherstellen von Oracle-Datenbanken                     | 982 |
| Klonen Sie die Oracle-Datenbanksicherung                                         | 985 |
| Verwalten von SnapCenter Server und Plug-Ins                                     | 988 |
| Dashboard anzeigen                                                               | 988 |
| Übersicht über das Dashboard                                                     | 988 |
| So zeigen Sie Informationen auf dem Dashboard an                                 | 992 |
| Fordern Sie Statusberichte der Jobs vom Dashboard an                             | 992 |
| Fordern Sie Berichte zum Schutzstatus vom Dashboard an                           | 993 |
| RBAC verwalten                                                                   | 993 |
| Ändern einer Rolle                                                               | 993 |
| Benutzer und Gruppen ändern                                                      | 994 |
| Hosts verwalten                                                                  | 994 |
| Aktualisieren der Informationen zur virtuellen Maschine                          | 996 |
| Plug-In-Hosts ändern                                                             | 997 |

|                                                                                    |      |
|------------------------------------------------------------------------------------|------|
| Starten oder Neustarten von Plug-In-Diensten .....                                 | 998  |
| Zeitpläne für Host-Wartung aussetzen .....                                         | 998  |
| Von der Seite „Ressourcen“ unterstützte Vorgänge .....                             | 999  |
| Richtlinien verwalten .....                                                        | 1000 |
| Richtlinien ändern .....                                                           | 1000 |
| Richtlinien trennen .....                                                          | 1001 |
| Richtlinien löschen .....                                                          | 1001 |
| Verwalten von Ressourcengruppen .....                                              | 1002 |
| Stoppen und Fortsetzen von Vorgängen für Ressourcengruppen .....                   | 1002 |
| Ressourcengruppen löschen .....                                                    | 1003 |
| Backups verwalten .....                                                            | 1003 |
| Backups umbenennen .....                                                           | 1003 |
| Backups löschen .....                                                              | 1004 |
| Schutz entfernen .....                                                             | 1004 |
| Klone löschen .....                                                                | 1005 |
| Überwachen Sie Jobs, Zeitpläne, Ereignisse und Protokolle .....                    | 1006 |
| Überwachen von Jobs .....                                                          | 1006 |
| Zeitpläne überwachen .....                                                         | 1007 |
| Überwachen von Ereignissen .....                                                   | 1007 |
| Überwachen von Protokollen .....                                                   | 1008 |
| Entfernen Sie Jobs und Protokolle aus SnapCenter .....                             | 1009 |
| Übersicht über die Berichtsfunktionen von SnapCenter .....                         | 1009 |
| Zugriffsberichte .....                                                             | 1011 |
| Filtern Sie Ihren Bericht .....                                                    | 1011 |
| Berichte exportieren oder drucken .....                                            | 1012 |
| SMTP-Server für E-Mail-Benachrichtigungen festlegen .....                          | 1012 |
| Konfigurieren Sie die Option zum Versenden von Berichten per E-Mail .....          | 1012 |
| Verwalten des SnapCenter Server-Repository .....                                   | 1013 |
| Voraussetzungen zum Schutz des SnapCenter -Repositorys .....                       | 1013 |
| Sichern Sie das SnapCenter Repository .....                                        | 1013 |
| Anzeigen von Backups des SnapCenter -Repositorys .....                             | 1014 |
| Wiederherstellen des SnapCenter -Datenbankrepositorys .....                        | 1014 |
| Migrieren des SnapCenter -Repositorys .....                                        | 1015 |
| Setzen Sie das Kennwort für das SnapCenter -Repository zurück .....                | 1015 |
| Verwalten von Ressourcen nicht vertrauenswürdiger Domänen .....                    | 1016 |
| Ändern nicht vertrauenswürdiger Domänen .....                                      | 1017 |
| Aufheben der Registrierung nicht vertrauenswürdiger Active Directory-Domänen ..... | 1017 |
| Verwalten des Speichersystems .....                                                | 1018 |
| Ändern der Speichersystemkonfiguration .....                                       | 1018 |
| Löschen Sie das Speichersystem .....                                               | 1020 |
| REST-API-Unterstützung .....                                                       | 1021 |
| Verwalten der EMS-Datenerfassung .....                                             | 1021 |
| Stoppen Sie die EMS-Datenerfassung .....                                           | 1021 |
| Starten Sie die EMS-Datenerfassung .....                                           | 1022 |
| Ändern Sie den Zeitplan für die EMS-Datenerfassung und das Ziel-SVM .....          | 1022 |



|                                                                                |      |
|--------------------------------------------------------------------------------|------|
| Überwachen Sie den Status der EMS-Datenerfassung .....                         | 1022 |
| Aktualisieren Sie SnapCenter Server und Plug-Ins .....                         | 1024 |
| Konfigurieren Sie SnapCenter , um nach verfügbaren Updates zu suchen .....     | 1024 |
| Upgrade-Workflow .....                                                         | 1024 |
| Unterstützte Upgradepfade .....                                                | 1024 |
| Aktualisieren Sie den SnapCenter -Server auf dem Windows-Host .....            | 1025 |
| Aktualisieren Sie den SnapCenter -Server auf dem Linux-Host .....              | 1027 |
| Aktualisieren Sie Ihre Plug-in-Pakete .....                                    | 1028 |
| Technische Aktualisierung .....                                                | 1031 |
| Technische Aktualisierung des SnapCenter Server-Hosts .....                    | 1031 |
| Technische Aktualisierung eines Knotens im F5-Cluster .....                    | 1032 |
| Außerbetriebnahme des alten SnapCenter Server-Hosts .....                      | 1032 |
| Rollback zum alten SnapCenter Server-Host .....                                | 1032 |
| Notfallwiederherstellung .....                                                 | 1032 |
| Technische Aktualisierung der SnapCenter -Plug-in-Hosts .....                  | 1034 |
| Technische Aktualisierung des Speichersystems .....                            | 1037 |
| Aktualisieren Sie die Backups des primären Speichers .....                     | 1037 |
| Aktualisieren Sie die Backups des sekundären Speichers .....                   | 1039 |
| Deinstallieren Sie SnapCenter Server und Plug-Ins .....                        | 1041 |
| Deinstallieren Sie SnapCenter Plug-In-Pakete .....                             | 1041 |
| Voraussetzungen für das Entfernen eines Hosts .....                            | 1041 |
| Einen Host entfernen .....                                                     | 1042 |
| Deinstallieren Sie Plug-Ins über die SnapCenter -GUI .....                     | 1043 |
| Deinstallieren Sie Windows-Plug-Ins mit dem PowerShell-Cmdlet .....            | 1044 |
| Plug-Ins lokal auf einem Host deinstallieren .....                             | 1044 |
| Deinstallieren Sie das Plug-In-Paket für Linux oder AIX mithilfe der CLI ..... | 1045 |
| Deinstallieren Sie den SnapCenter -Server auf dem Windows-Host .....           | 1045 |
| Deinstallieren Sie den SnapCenter -Server auf dem Linux-Host .....             | 1046 |
| Automatisieren Sie mit REST-APIs .....                                         | 1047 |
| SnapCenter -Automatisierung mithilfe von REST-APIs .....                       | 1047 |
| So greifen Sie nativ auf die SnapCenter REST-API zu .....                      | 1047 |
| REST-Webdienstgrundlagen .....                                                 | 1047 |
| Ressourcen und staatliche Vertretung .....                                     | 1047 |
| URI-Endpunkte .....                                                            | 1048 |
| HTTP-Nachrichten .....                                                         | 1048 |
| JSON-Formatierung .....                                                        | 1048 |
| Grundlegende Betriebsmerkmale .....                                            | 1048 |
| Anforderungs- und Antwort-API-Transaktion .....                                | 1048 |
| Unterstützung für CRUD-Operationen .....                                       | 1048 |
| Objektkennungen .....                                                          | 1049 |
| Objektinstanzen und Sammlungen .....                                           | 1049 |
| Synchrone und asynchrone Vorgänge .....                                        | 1049 |
| Sicherheit .....                                                               | 1049 |
| Eingabevariablen, die eine API-Anfrage steuern .....                           | 1050 |
| HTTP-Methoden .....                                                            | 1050 |

|                                                                |      |
|----------------------------------------------------------------|------|
| Anforderungsheader                                             | 1050 |
| Anforderungstext                                               | 1051 |
| Objekte filtern                                                | 1051 |
| Anfordern bestimmter Objektfelder                              | 1051 |
| Sortieren von Objekten im Ausgabesatz                          | 1052 |
| Seitennummerierung beim Abrufen von Objekten in einer Sammlung | 1052 |
| Größeneigenschaften                                            | 1053 |
| Interpretation einer API-Antwort                               | 1053 |
| HTTP-Statuscode                                                | 1053 |
| Antwortheader                                                  | 1054 |
| Antworttext                                                    | 1054 |
| Fehler                                                         | 1055 |
| Für SnapCenter Server und Plug-Ins unterstützte REST-APIs      | 1056 |
| Authentifizierung                                              | 1056 |
| Domänen                                                        | 1056 |
| Jobs                                                           | 1056 |
| Einstellungen                                                  | 1056 |
| Gastgeber                                                      | 1057 |
| Ressourcen                                                     | 1057 |
| Backups                                                        | 1059 |
| Klone                                                          | 1059 |
| Klonaufteilung                                                 | 1060 |
| Ressourcengruppen                                              | 1060 |
| Richtlinien                                                    | 1060 |
| Storage                                                        | 1060 |
| Aktie                                                          | 1061 |
| Plugins                                                        | 1061 |
| Berichte                                                       | 1062 |
| Warnungen                                                      | 1062 |
| Rbac                                                           | 1062 |
| Konfiguration                                                  | 1063 |
| Zertifikateinstellungen                                        | 1063 |
| Archiv                                                         | 1063 |
| Version                                                        | 1063 |
| So greifen Sie über die Swagger-API-Webseite auf REST-APIs zu  | 1063 |
| Erste Schritte mit der REST-API                                | 1064 |
| Hallo Welt                                                     | 1064 |
| Rechtliche Hinweise                                            | 1066 |
| Copyright                                                      | 1066 |
| Marken                                                         | 1066 |
| Patente                                                        | 1066 |
| Datenschutzrichtlinie                                          | 1066 |
| Open Source                                                    | 1066 |

# SnapCenter software Softwaredokumentation

# Versionshinweise

## Versionshinweise

Informieren Sie sich über die neuen und verbesserten Funktionen in SnapCenter 6.1.

Eine vollständige Liste der neuen Funktionen und Verbesserungen finden Sie unter ["Was ist neu in SnapCenter 6.1"](#) .

Einzelheiten zu bekannten Problemen, Einschränkungen, behobenen Problemen sowie neuen und geänderten Befehlen finden Sie im ["Versionshinweise zur SnapCenter -Software 6.1"](#) . Sie müssen sich mit Ihrem NetApp -Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zugreifen zu können.

## Unterstützte Upgradepfade für SnapCenter

Der Upgradepfad hilft Ihnen zu verstehen, von welchen früheren Versionen von SnapCenter Sie auf die neuesten Versionen von SnapCenter aktualisieren können und welche Versionen der Plug-Ins unterstützt werden.

| Wenn Sie die SnapCenter Server-Version verwenden ... | Sie können SnapCenter Server direkt aktualisieren auf... | Unterstützte Plug-in-Versionen                                        |
|------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------------------------|
| 5,0                                                  | 6,0                                                      | <ul style="list-style-type: none"><li>• 5,0</li><li>• 6,0</li></ul>   |
|                                                      | 6.0.1                                                    | <ul style="list-style-type: none"><li>• 6.0.1</li></ul>               |
|                                                      | 6,1                                                      | <ul style="list-style-type: none"><li>• 6,1</li></ul>                 |
| 6,0                                                  | 6.0.1                                                    | <ul style="list-style-type: none"><li>• 6,0</li><li>• 6.0.1</li></ul> |
|                                                      | 6,1                                                      | <ul style="list-style-type: none"><li>• 6,1</li></ul>                 |
| 6.0.1                                                | 6,1                                                      | <ul style="list-style-type: none"><li>• 6.0.1</li><li>• 6,1</li></ul> |

Informationen zum Upgrade des SnapCenter Plug-in for VMware vSphere finden Sie unter ["Aktualisieren Sie das SnapCenter Plug-in for VMware vSphere"](#) .

# Erste Schritte

## Erfahren Sie mehr über die SnapCenter software

### SnapCenter -Übersicht

Die SnapCenter software ist eine einfache, zentralisierte und skalierbare Plattform für anwendungskonsistenten Datenschutz. Es schützt Anwendungen, Datenbanken, Host-Dateisysteme und VMs auf ONTAP -Systemen in der Hybrid Cloud.

SnapCenter verwendet die Technologien NetApp Snapshot, SnapRestore, FlexClone, SnapMirror und SnapVault , um Folgendes bereitzustellen:

- Schnelle, platzsparende, anwendungskonsistente, festplattenbasierte Backups
- Schnelle, detaillierte Wiederherstellung und anwendungskonsistente Wiederherstellung
- Schnelles, platzsparendes Klonen

SnapCenter umfasst SnapCenter Server und leichte Plug-Ins. Sie können die Plug-In-Bereitstellung auf Remote-Anwendungshosts automatisieren, Sicherungs-, Überprüfungs- und Klonvorgänge planen und Datenschutzvorgänge überwachen.

Sie können SnapCenter zum Schutz Ihrer Daten entweder vor Ort oder in einer öffentlichen Cloud installieren.

- Vor Ort zum Schutz der folgenden Punkte:
  - Daten, die sich auf primären ONTAP FAS, AFF oder ASA Systemen befinden und auf sekundäre ONTAP FAS, AFF oder ASA Systeme repliziert werden
  - Daten, die sich auf primären ONTAP Select Systemen befinden
  - Daten, die sich auf primären und sekundären ONTAP FAS, AFF oder ASA -Systemen befinden und durch den lokalen StorageGRID Objektspeicher geschützt sind
  - Daten, die sich auf primären und sekundären ONTAP ASA r2-Systemen befinden
- Vor Ort in einer Hybrid Cloud zum Schutz der folgenden Elemente:
  - Daten, die sich auf primären ONTAP FAS, AFF oder ASA Systemen befinden und auf Cloud Volumes ONTAP repliziert werden
  - Daten, die sich auf primären und sekundären ONTAP FAS, AFF oder ASA -Systemen befinden und durch Objekt- und Archivspeicher in der Cloud geschützt sind (mithilfe der BlueXP backup and recovery )
- In einer öffentlichen Cloud zum Schutz der folgenden Elemente:
  - Daten, die sich auf primären Systemen von Cloud Volumes ONTAP (früher ONTAP Cloud) befinden
  - Daten, die sich auf Amazon FSX für ONTAP befinden
  - Daten, die sich auf primären Azure NetApp Files (Oracle, Microsoft SQL und SAP HANA) befinden

### Hauptmerkmale

SnapCenter bietet die folgenden Hauptfunktionen:

- Zentralisierter, anwendungskonsistenter Datenschutz verschiedener Anwendungen

Der Datenschutz wird für Microsoft Exchange Server, Microsoft SQL Server, Oracle-Datenbanken unter Linux oder AIX, SAP HANA-Datenbanken, IBM Db2, PostgreSQL, MySQL und Windows-Host-Dateisysteme unterstützt, die auf ONTAP Systemen ausgeführt werden. SnapCenter unterstützt auch den Schutz von Anwendungen wie MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Richtlinienbasierte Backups

Richtlinienbasierte Backups nutzen die NetApp Snapshot-Technologie, um schnelle, platzsparende, anwendungskonsistente, festplattenbasierte Backups zu erstellen. Sie können auch einen automatischen Schutz dieser Sicherungen auf einem sekundären Speicher einrichten, indem Sie vorhandene Schutzbeziehungen aktualisieren.

- Backups für mehrere Ressourcen

Mithilfe von SnapCenter -Ressourcengruppen können Sie mehrere Ressourcen (Anwendungen, Datenbanken oder Hostdateisysteme) desselben Typs gleichzeitig sichern.

- Wiederherstellung und Wiederherstellung

SnapCenter ermöglicht schnelle, granulare Wiederherstellungen von Backups und anwendungskonsistente, zeitbasierte Wiederherstellung. Sie können von jedem Ziel in der Hybrid Cloud wiederherstellen.

- Klonen

SnapCenter ermöglicht schnelles, platzsparendes und anwendungskonsistentes Klonen. Sie können auf jedem Ziel in der Hybrid Cloud klonen.

- Grafische Benutzeroberfläche für die Einzelbenutzerverwaltung

SnapCenter bietet eine einzige Schnittstelle zum Verwalten von Backups und Klonen in jedem Hybrid Cloud-Ziel.

- REST-APIs, Windows-Cmdlets, UNIX-Befehle

SnapCenter bietet REST-APIs für die meisten Funktionen zur Integration mit jeder Orchestrierungssoftware sowie zur Verwendung von Windows PowerShell-Cmdlets und der Befehlszeilenschnittstelle.

- Zentralisiertes Datenschutz-Dashboard und Reporting

- Rollenbasierte Zugriffskontrolle (RBAC) für Sicherheit und Delegation

- Eine integrierte Repository-Datenbank mit hoher Verfügbarkeit zum Speichern aller Backup-Metadaten

- Automatisierte Push-Installation von Plug-Ins

- Hohe Verfügbarkeit

- Notfallwiederherstellung (DR)

- SnapLock "[Weitere Informationen](#)"

- SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC])

- Synchrone Spiegelung "[Weitere Informationen](#)"

## **SnapCenter -Architektur und -Komponenten**

SnapCenter verwendet ein mehrschichtiges Design mit einem zentralen Verwaltungsserver und Plug-in-Hosts. Die Server- und Plug-In-Hosts können sich an verschiedenen Standorten befinden.

SnapCenter umfasst den SnapCenter Server, das SnapCenter Plug-In-Paket für Windows und das SnapCenter Plug-In-Paket für Linux. Jedes Paket enthält Plug-Ins für verschiedene Anwendungen und Infrastrukturkomponenten.

### SnapCenter Server

Der SnapCenter Server unterstützt die Betriebssysteme Microsoft Windows und Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Der SnapCenter -Server umfasst einen Webserver, eine zentralisierte HTML5-basierte Benutzeroberfläche, PowerShell-Cmdlets, REST-APIs und das SnapCenter Repository.

SnapCenter speichert Informationen zu seinen Vorgängen im SnapCenter -Repository.

### SnapCenter -Plug-Ins

Jedes SnapCenter Plug-in unterstützt bestimmte Umgebungen, Datenbanken und Anwendungen.

| Plug-in-Name                                      | Im Installationspaket enthalten                       | Erfordert andere Plug-Ins                 | Auf dem Host installiert | Unterstützte Plattform  |
|---------------------------------------------------|-------------------------------------------------------|-------------------------------------------|--------------------------|-------------------------|
| SnapCenter -Plug-In für Microsoft SQL Server      | Plug-In-Paket für Windows                             | Plug-in für Windows                       | SQL Server-Host          | Windows                 |
| SnapCenter -Plug-in für Windows                   | Plug-In-Paket für Windows                             |                                           | Windows-Host             | Windows                 |
| SnapCenter -Plug-in für Microsoft Exchange Server | Plug-In-Paket für Windows                             | Plug-in für Windows                       | Exchange Server-Host     | Windows                 |
| SnapCentre-Plug-in für Oracle-Datenbank           | Plug-In-Paket für Linux und Plug-In-Paket für AIX     | Plug-in für UNIX                          | Oracle-Host              | Linux oder AIX          |
| SnapCenter Plug-in für SAP HANA-Datenbank         | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | HDBSQL-Client-Host       | Linux oder Windows      |
| SnapCenter -Plug-in für IBM Db2                   | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | Db2-Host                 | Linux, AIX oder Windows |
| SnapCenter -Plug-in für PostgreSQL                | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | PostgreSQL-Host          | Linux oder Windows      |
| SnaoCenter-Plug-in für MySQL                      | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | MySQL-Host               | Linux oder Windows      |

| Plug-in-Name                                         | Im Installationspaket enthalten                       | Erfordert andere Plug-Ins                 | Auf dem Host installiert | Unterstützte Plattform |
|------------------------------------------------------|-------------------------------------------------------|-------------------------------------------|--------------------------|------------------------|
| SnapCenter -Plug-in für MongoDB                      | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | MongoDB-Host             | Linux oder Windows     |
| SnapCenter -Plug-in für ORASCPM (Oracle-Anwendungen) | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | Oracle-Host              | Linux oder Windows     |
| SnapCenter Plug-In für SAP ASE                       | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | SAP-Host                 | Linux oder Windows     |
| SnapCenter -Plug-in für SAP MaxDB                    | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | SAP MaxDB-Host           | Linux oder Windows     |
| SnapCenter -Plug-in für Speicher-Plug-in             | Plug-In-Paket für Linux und Plug-In-Paket für Windows | Plug-in für UNIX oder Plug-in für Windows | Speicherhost             | Linux oder Windows     |

Das SnapCenter Plug-in for VMware vSphere unterstützt absturzkonsistente und VM-konsistente Sicherungs- und Wiederherstellungsvorgänge für virtuelle Maschinen (VMs), Datenspeicher und Virtual Machine Disks (VMDKs). Es unterstützt außerdem anwendungskonsistente Sicherungs- und Wiederherstellungsvorgänge für virtualisierte Datenbanken und Dateisysteme.

Um Datenbanken, Dateisysteme, VMs oder Datenspeicher auf VMs zu schützen, stellen Sie das SnapCenter Plug-in for VMware vSphere Geräte bereit. Weitere Informationen finden Sie unter ["SnapCenter Plug-in for VMware vSphere Dokumentation"](#) .

### SnapCenter -Repository

Das SnapCenter Repository, manchmal auch als NSM-Datenbank bezeichnet, speichert Informationen und Metadaten für jeden SnapCenter Vorgang.

Bei der SnapCenter Server-Installation wird standardmäßig die MySQL Server-Repository-Datenbank installiert. Wenn Sie MySQL Server bereits installiert haben und eine Neuinstallation von SnapCenter Server durchführen möchten, müssen Sie MySQL Server deinstallieren.

SnapCenter unterstützt MySQL Server 8.0.37 oder höher als SnapCenter -Repository-Datenbank. Wenn Sie eine frühere Version von MySQL Server mit einer früheren Version von SnapCenter verwenden, aktualisiert der SnapCenter -Upgradeprozess MySQL Server auf Version 8.0.37 oder höher.

Das SnapCenter -Repository speichert die folgenden Informationen und Metadaten:

- Metadaten sichern, klonen, wiederherstellen und überprüfen
- Berichts-, Job- und Ereignisinformationen



- Host- und Plug-in-Informationen
- Rollen-, Benutzer- und Berechtigungsdetails
- Informationen zur Speichersystemverbindung

## Sicherheitsfunktionen in SnapCenter

SnapCenter verwendet strenge Sicherheits- und Authentifizierungsfunktionen, damit Ihre Daten geschützt bleiben.

SnapCenter umfasst die folgenden Sicherheitsfunktionen:

- Die gesamte Kommunikation mit SnapCenter erfolgt über HTTP über SSL (HTTPS).
- Alle Anmeldeinformationen in SnapCenter sind durch die Verschlüsselung Advanced Encryption Standard (AES) geschützt.
- Unterstützt Sicherheitsalgorithmen, die dem Federal Information Processing Standard (FIPS) entsprechen.
- Unterstützt die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.
- Unterstützt Transport Layer Security (TLS) 1.3 für die Kommunikation mit ONTAP. Sie können TLS 1.2 auch für die Kommunikation zwischen Clients und Servern verwenden.
- Unterstützt einen bestimmten Satz von SSL-Verschlüsselungssammlungen, um Sicherheit bei der Netzwerkkommunikation zu gewährleisten. ["Mehr erfahren"](#) .
- SnapCenter wird innerhalb der Firewall Ihres Unternehmens installiert, um den Zugriff auf den SnapCenter -Server und die Kommunikation zwischen dem SnapCenter -Server und den Plug-Ins zu ermöglichen.
- Für den Zugriff auf die SnapCenter -API und -Operationen werden mit AES-Verschlüsselung verschlüsselte Token verwendet, die nach 24 Stunden ablaufen.
- SnapCenter lässt sich in Windows Active Directory integrieren, um die Anmeldung und die rollenbasierte Zugriffskontrolle (RBAC) zu ermöglichen, die die Zugriffsberechtigungen regelt.
- IPsec wird mit SnapCenter auf ONTAP für Windows- und Linux-Hostmaschinen unterstützt. ["Mehr erfahren"](#) .
- SnapCenter PowerShell-Cmdlets sind sitzungsgesichert.
- Nach einer standardmäßigen Inaktivitätszeit von 15 Minuten warnt Sie SnapCenter , dass Sie in 5 Minuten abgemeldet werden.

Nach 20 Minuten Inaktivität meldet SnapCenter Sie ab und Sie müssen sich erneut anmelden. Sie können den Abmeldezeitraum ändern.

- Nach 5 falschen Anmeldeversuchen wird die Anmeldung vorübergehend deaktiviert.
- Unterstützt die CA-Zertifikatauthentifizierung zwischen SnapCenter Server und ONTAP. ["Mehr erfahren"](#) .
- Integrity Verifier wird dem SnapCenter -Server und den Plug-Ins hinzugefügt und validiert alle mitgelieferten Binärdateien während Neuinstallations- und Upgradevorgängen.

## CA-Zertifikatübersicht

Das SnapCenter Server-Installationsprogramm aktiviert während der Installation die zentrale SSL-Zertifikatunterstützung. Um die sichere Kommunikation zwischen dem Server und dem Plug-in zu verbessern, unterstützt SnapCenter die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.

Sie sollten CA-Zertifikate nach der Installation des SnapCenter -Servers und der entsprechenden Plug-Ins

bereitstellen. Weitere Informationen finden Sie unter ["CA-Zertifikat-CSR-Datei generieren"](#) .

Sie können auch ein CA-Zertifikat für das SnapCenter -Plug-In für VMware vSphere bereitstellen. Weitere Informationen finden Sie unter ["Zertifikate erstellen und importieren"](#) .

## **Zweiwege-SSL-Kommunikation**

Die bidirektionale SSL-Kommunikation sichert die gegenseitige Kommunikation zwischen SnapCenter Server und den Plug-Ins.

## **Übersicht über die zertifikatbasierte Authentifizierung**

Die zertifikatsbasierte Authentifizierung überprüft die Authentizität der jeweiligen Benutzer, die versuchen, auf den SnapCenter -Plug-In-Host zuzugreifen. Der Benutzer sollte das SnapCenter -Server-Zertifikat ohne privaten Schlüssel exportieren und in den vertrauenswürdigen Speicher des Plug-In-Hosts importieren. Die zertifikatsbasierte Authentifizierung funktioniert nur, wenn die bidirektionale SSL-Funktion aktiviert ist.

## **Multi-Faktor-Authentifizierung (MFA)**

MFA verwendet einen Identitätsanbieter (IdP) eines Drittanbieters über die Security Assertion Markup Language (SAML), um Benutzersitzungen zu verwalten. Diese Funktion verbessert die Authentifizierungssicherheit durch die Möglichkeit, neben dem vorhandenen Benutzernamen und Kennwort mehrere Faktoren wie TOTP, Biometrie, Push-Benachrichtigungen usw. zu verwenden. Darüber hinaus ermöglicht es dem Kunden, seine eigenen Benutzeridentitätsanbieter zu verwenden, um eine einheitliche Benutzeranmeldung (SSO) für sein gesamtes Portfolio zu erhalten.

MFA ist nur für die Anmeldung bei der SnapCenter Server-Benutzeroberfläche anwendbar. Die Anmeldungen werden über die IdP Active Directory Federation Services (AD FS) authentifiziert. Sie können bei AD FS verschiedene Authentifizierungsfaktoren konfigurieren. SnapCenter ist der Dienstanbieter und Sie sollten SnapCenter als vertrauende Partei in AD FS konfigurieren. Um MFA in SnapCenter zu aktivieren, benötigen Sie die AD FS-Metadaten.

Informationen zum Aktivieren von MFA finden Sie unter ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#) .

## **Rollenbasierte Zugriffskontrolle in SnapCenter**

Die rollenbasierte Zugriffskontrolle (RBAC) und ONTAP Berechtigungen von SnapCenter ermöglichen es SnapCenter Administratoren, die Kontrolle über SnapCenter -Ressourcen an verschiedene Benutzer oder Benutzergruppen zu delegieren. Dieser zentral verwaltete Zugriff ermöglicht Anwendungsadministratoren, sicher in delegierten Umgebungen zu arbeiten.

Sie können jederzeit Rollen erstellen und ändern und Benutzern Ressourcenzugriff gewähren. Wenn Sie SnapCenter jedoch zum ersten Mal einrichten, sollten Sie zumindest Active Directory-Benutzer oder -Gruppen zu Rollen hinzufügen und diesen Benutzern oder Gruppen dann Ressourcenzugriff gewähren.



Sie können SnapCenter nicht zum Erstellen von Benutzer- oder Gruppenkonten verwenden. Sie sollten Benutzer- oder Gruppenkonten im Active Directory des Betriebssystems oder der Datenbank erstellen.

## Arten von RBAC in SnapCenter

SnapCenter verwendet die folgenden Arten der rollenbasierten Zugriffskontrolle:

- SnapCenter RBAC
- RBAC auf Anwendungsebene
- SnapCenter -Plug-in für VMware vSphere RBAC
- ONTAP-Berechtigungen

### SnapCenter RBAC

SnapCenter verfügt über vordefinierte Rollen und Sie können diesen Rollen Benutzer oder Benutzergruppen zuweisen. Die vordefinierten Rollen sind:

- SnapCenter -Administratorrolle
- Rolle „App-Backup und -Klon-Administrator“
- Rolle „Backup- und Klon-Viewer“
- Rolle des Infrastrukturadministrators

Wenn Sie einem Benutzer eine Rolle zuweisen, werden auf der Seite „Jobs“ nur die für diesen Benutzer relevanten Jobs angezeigt, es sei denn, Sie haben ihm die Rolle „SnapCenterAdmin“ zugewiesen.

Sie können auch neue Rollen erstellen und Berechtigungen und Benutzer verwalten. Sie können Benutzern oder Gruppen Berechtigungen für den Zugriff auf SnapCenter -Objekte wie Hosts, Speicherverbindungen und Ressourcengruppen zuweisen.

Sie können Benutzern und Gruppen innerhalb derselben Gesamtstruktur und Benutzern, die zu verschiedenen Gesamtstrukturen gehören, RBAC-Berechtigungen zuweisen. Sie können Benutzern, die zu verschachtelten Gruppen gehören, keine RBAC-Berechtigungen über Gesamtstrukturen hinweg zuweisen.



Wenn Sie eine benutzerdefinierte Rolle erstellen, muss diese alle Berechtigungen der SnapCenterAdmin-Rolle enthalten. Wenn Sie nur einige der Berechtigungen kopieren, beispielsweise „Host hinzufügen“ oder „Host entfernen“, können Sie diese Vorgänge nicht ausführen.

Benutzer müssen sich bei der Anmeldung über die grafische Benutzeroberfläche (GUI) oder mithilfe von PowerShell-Cmdlets authentifizieren. Wenn Benutzer Mitglieder mehrerer Rollen sind, werden sie nach der Eingabe der Anmeldeinformationen aufgefordert, die Rolle anzugeben, die sie verwenden möchten. Benutzer müssen sich außerdem authentifizieren, um die APIs auszuführen.

### RBAC auf Anwendungsebene

SnapCenter verwendet Anmeldeinformationen, um zu überprüfen, ob autorisierte SnapCenter Benutzer auch über Berechtigungen auf Anwendungsebene verfügen.

Wenn Sie beispielsweise Datenschutzvorgänge in einer SQL Server-Umgebung durchführen möchten, müssen Sie die Anmeldeinformationen mit den richtigen Windows- oder SQL-Anmeldeinformationen festlegen. Der SnapCenter -Server authentifiziert die festgelegten Anmeldeinformationen mit einer der beiden Methoden. Wenn Sie Datenschutzvorgänge in einer Windows-Dateisystemumgebung auf ONTAP -Speicher durchführen möchten, muss die SnapCenter Administratorrolle über Administratorrechte auf dem Windows-Host verfügen.

Wenn Sie Datenschutzvorgänge für eine Oracle-Datenbank durchführen möchten und die

Betriebssystemauthentifizierung im Datenbankhost deaktiviert ist, müssen Sie die Anmeldeinformationen mit den Anmeldeinformationen der Oracle-Datenbank oder von Oracle ASM festlegen. Der SnapCenter -Server authentifiziert die festgelegten Anmeldeinformationen je nach Vorgang mit einer dieser Methoden.

### SnapCenter Plug-in for VMware vSphere RBAC

Wenn Sie das SnapCenter VMware-Plug-In für VM-konsistenten Datenschutz verwenden, bietet der vCenter Server eine zusätzliche RBAC-Ebene. Das SnapCenter VMware-Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC. ["Weitere Informationen"](#)

**Best Practice:** NetApp empfiehlt, dass Sie eine ONTAP Rolle für SnapCenter Plug-in for VMware vSphere Vorgänge erstellen und ihr alle erforderlichen Berechtigungen zuweisen.

### ONTAP-Berechtigungen

Sie sollten ein vsadmin-Konto mit den erforderlichen Berechtigungen für den Zugriff auf das Speichersystem erstellen. ["Weitere Informationen"](#)

### Den vordefinierten SnapCenter -Rollen zugewiesene Berechtigungen

Wenn Sie einen Benutzer zu einer Rolle hinzufügen, müssen Sie entweder die Berechtigung „StorageConnection“ zuweisen, um die Kommunikation mit der Storage Virtual Machine (SVM) zu ermöglichen, oder dem Benutzer eine SVM zuweisen, um die Berechtigung zur Verwendung der SVM zu aktivieren. Mit der Berechtigung „Speicherverbindung“ können Benutzer SVM-Verbindungen erstellen.

Beispielsweise kann ein Benutzer mit der SnapCenter -Administratorrolle SVM-Verbindungen erstellen und sie einem Benutzer mit der Rolle „App Backup and Clone Admin“ zuweisen, der standardmäßig nicht über die Berechtigung zum Erstellen oder Bearbeiten von SVM-Verbindungen verfügt. Ohne eine SVM-Verbindung können Benutzer keine Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen.

### SnapCenter -Administratorrolle

Für die SnapCenter Administratorrolle sind alle Berechtigungen aktiviert. Sie können die Berechtigungen für diese Rolle nicht ändern. Sie können der Rolle Benutzer und Gruppen hinzufügen oder sie entfernen.

### Rolle „App-Backup und -Klon-Administrator“

Die Rolle „App-Backup- und -Klon-Administrator“ verfügt über die erforderlichen Berechtigungen zum Ausführen administrativer Aktionen für Anwendungs-Backups und klonbezogene Aufgaben. Diese Rolle verfügt nicht über Berechtigungen für Hostverwaltung, Bereitstellung, Speicherverbindungsverwaltung oder Remoteinstallation.

| Berechtigungen   | Ermöglicht       | Erstellen | Lesen | Aktualisieren | Löschen |
|------------------|------------------|-----------|-------|---------------|---------|
| Ressourcengruppe | Nicht zutreffend | Ja        | Ja    | Ja            | Ja      |
| Politik          | Nicht zutreffend | Ja        | Ja    | Ja            | Ja      |
| Sicherung        | Nicht zutreffend | Ja        | Ja    | Ja            | Ja      |
| Gastgeber        | Nicht zutreffend | Ja        | Ja    | Ja            | Ja      |

| <b>Berechtigungen</b>                 | <b>Ermöglicht</b> | <b>Erstellen</b> | <b>Lesen</b>     | <b>Aktualisieren</b> | <b>Löschen</b>   |
|---------------------------------------|-------------------|------------------|------------------|----------------------|------------------|
| Speicherverbindung                    | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Klonen                                | Nicht zutreffend  | Ja               | Ja               | Ja                   | Ja               |
| Bestimmung                            | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Dashboard                             | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Berichte                              | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Wiederherstellen                      | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Ressource                             | Ja                | Ja               | Ja               | Ja                   | Ja               |
| Plug-in installieren/deinstallieren   | Nein              | Nicht zutreffend |                  | Nicht zutreffend     | Nicht zutreffend |
| Migration                             | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Montieren                             | Ja                | Ja               | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Aushängen                             | Ja                | Ja               | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Vollständige Volume-Wiederherstellung | Nein              | Nein             | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Sekundärschutz                        | Nein              | Nein             | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Job-Monitor                           | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |

#### **Rolle „Backup- und Klon-Viewer“**

Die Rolle „Backup- und Klon-Viewer“ verfügt über schreibgeschützte Ansicht aller Berechtigungen. Für diese Rolle sind außerdem Berechtigungen für die Erkennung, Berichterstellung und den Zugriff auf das Dashboard aktiviert.

| <b>Berechtigungen</b> | <b>Ermöglicht</b> | <b>Erstellen</b> | <b>Lesen</b> | <b>Aktualisieren</b> | <b>Löschen</b> |
|-----------------------|-------------------|------------------|--------------|----------------------|----------------|
| Ressourcengruppe      | Nicht zutreffend  | Nein             | Ja           | Nein                 | Nein           |

| <b>Berechtigungen</b>                 | <b>Ermöglicht</b> | <b>Erstellen</b> | <b>Lesen</b>     | <b>Aktualisieren</b> | <b>Löschen</b>   |
|---------------------------------------|-------------------|------------------|------------------|----------------------|------------------|
| Politik                               | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Sicherung                             | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Gastgeber                             | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Speicherverbindung                    | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Klonen                                | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Bestimmung                            | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Dashboard                             | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Berichte                              | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Wiederherstellen                      | Nein              | Nein             | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Ressource                             | Nein              | Nein             | Ja               | Ja                   | Nein             |
| Plug-in installieren/deinstallieren   | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Migration                             | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Montieren                             | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Aushängen                             | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Vollständige Volume-Wiederherstellung | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Sekundärschutz                        | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Job-Monitor                           | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |

#### **Rolle des Infrastrukturadministrators**

Die Rolle „Infrastrukturadministrator“ verfügt über Berechtigungen für Hostverwaltung, Speicherverwaltung, Bereitstellung, Ressourcengruppen, Remote-Installationsberichte und Zugriff auf das Dashboard.

| <b>Berechtigungen</b>                 | <b>Ermöglicht</b> | <b>Erstellen</b> | <b>Lesen</b>     | <b>Aktualisieren</b> | <b>Löschen</b>   |
|---------------------------------------|-------------------|------------------|------------------|----------------------|------------------|
| Ressourcengruppe                      | Nicht zutreffend  | Ja               | Ja               | Ja                   | Ja               |
| Politik                               | Nicht zutreffend  | Nein             | Ja               | Ja                   | Ja               |
| Sicherung                             | Nicht zutreffend  | Ja               | Ja               | Ja                   | Ja               |
| Gastgeber                             | Nicht zutreffend  | Ja               | Ja               | Ja                   | Ja               |
| Speicherverbindung                    | Nicht zutreffend  | Ja               | Ja               | Ja                   | Ja               |
| Klonen                                | Nicht zutreffend  | Nein             | Ja               | Nein                 | Nein             |
| Bestimmung                            | Nicht zutreffend  | Ja               | Ja               | Ja                   | Ja               |
| Dashboard                             | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Berichte                              | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Wiederherstellen                      | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Ressource                             | Ja                | Ja               | Ja               | Ja                   | Ja               |
| Plug-in installieren/deinstallieren   | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Migration                             | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Montieren                             | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Aushängen                             | Nein              | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Vollständige Volume-Wiederherstellung | Nein              | Nein             | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Sekundärschutz                        | Nein              | Nein             | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |
| Job-Monitor                           | Ja                | Nicht zutreffend | Nicht zutreffend | Nicht zutreffend     | Nicht zutreffend |

## Notfallwiederherstellung in SnapCenter

Mit der Disaster Recovery-Funktion (DR) von SnapCenter können Sie sich von Katastrophen wie Ressourcenbeschädigungen oder Serverabstürzen erholen. Es hilft bei der Wiederherstellung des SnapCenter Repositorys, der Serverpläne, der Konfigurationskomponenten und des SnapCenter -Plug-ins für SQL Server und seines Speichers.

In diesem Abschnitt werden die beiden Arten von DR in SnapCenter erläutert:

### SnapCenter Server DR

- SnapCenter Server-Daten werden gesichert und können wiederhergestellt werden, ohne dass dem SnapCenter Server ein Plug-In hinzugefügt oder von diesem verwaltet werden muss.
- Der sekundäre SnapCenter -Server sollte im selben Installationsverzeichnis und auf demselben Port wie der primäre SnapCenter -Server installiert werden.
- Schließen Sie für die Multi-Faktor-Authentifizierung (MFA) während der SnapCenter Server-DR alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um sich erneut anzumelden. Dadurch werden die vorhandenen oder aktiven Sitzungscookies gelöscht und die richtigen Konfigurationsdaten aktualisiert.
- Die Notfallwiederherstellungsfunktion von SnapCenter verwendet REST-APIs zum Sichern des SnapCenter -Servers. Sehen ["REST-API-Workflows für die Notfallwiederherstellung von SnapCenter Server"](#) .
- Die Konfigurationsdatei mit den Überwachungseinstellungen wird weder im DR-Backup noch auf dem DR-Server nach dem Wiederherstellungsvorgang gesichert. Sie sollten die Audit-Protokolleinstellungen manuell wiederholen.

### SnapCenter Plug-in und Storage DR

DR ist nur für das SnapCenter -Plug-in für SQL Server verfügbar. Wenn das Plug-In ausgefallen ist, wechseln Sie zu einem anderen SQL-Host und stellen Sie die Daten mithilfe einiger Schritte wieder her. Sehen ["Notfallwiederherstellung des SnapCenter -Plug-ins für SQL Server"](#) .

SnapCenter verwendet ONTAP SnapMirror zum Replizieren von Daten, was für DR verwendet werden kann, indem die Daten an einem sekundären Standort synchronisiert bleiben. Um ein Failover einzuleiten, unterbrechen Sie die SnapMirror -Replikation. Kehren Sie während des Fallbacks die Synchronisierung um, um Daten vom DR-Standort zurück zum primären Standort zu replizieren.

## Von SnapCenter benötigte Lizenzen

SnapCenter erfordert mehrere Lizenzen, um den Datenschutz von Anwendungen, Datenbanken, Dateisystemen und virtuellen Maschinen zu ermöglichen. Die Art der SnapCenter -Lizenzen, die Sie installieren, hängt von Ihrer Speicherumgebung und den Funktionen ab, die Sie verwenden möchten.



| Lizenz                                        | Wo erforderlich                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>SnapCenter Standard-Controller-basiert</p> | <p>Erforderlich für FAS, AFF, ASA</p> <p>Die SnapCenter Standard-Lizenz ist eine Controller-basierte Lizenz und ist Teil von NetApp ONTAP One. Wenn Sie über die SnapManager Suite-Lizenz verfügen, erhalten Sie auch die SnapCenter Standard-Lizenzberechtigung. Wenn Sie SnapCenter auf Testbasis mit FAS, AFF oder ASA -Speicher installieren möchten, können Sie eine Evaluierungslizenz für NetApp ONTAP One erhalten, indem Sie sich an den Vertriebsmitarbeiter wenden.</p> <p>Informationen zu den in NetApp ONTAP One enthaltenen Lizenzen finden Sie unter <a href="#">"In NetApp ONTAP One enthaltene Lizenzen"</a> .</p> <div data-bbox="849 764 904 819">  </div> <p>SnapCenter wird auch als Teil eines Datenschutzpakets angeboten. Wenn Sie A400 oder höher gekauft haben, sollten Sie das Datenschutzpaket erwerben.</p> |
| <p>SnapMirror oder SnapVault</p>              | <p>ONTAP</p> <p>Wenn die Replikation in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault -Lizenz erforderlich.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>SnapRestore</p>                            | <p>Erforderlich zum Wiederherstellen und Überprüfen von Sicherungen.</p> <p>Auf primären Speichersystemen</p> <ul style="list-style-type: none"> <li>• Erforderlich auf SnapVault -Zielsystemen, um eine Remote-Überprüfung durchzuführen und aus einer Sicherung wiederherzustellen.</li> <li>• Erforderlich auf SnapMirror Zielsystemen, um eine Remote-Verifizierung durchzuführen.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Lizenz                                  | Wo erforderlich                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FlexClone                               | <p>Erforderlich zum Klonen von Datenbanken und für Überprüfungsvorgänge.</p> <p>Auf primären und sekundären Speichersystemen</p> <ul style="list-style-type: none"> <li>• Erforderlich auf SnapVault -Zielsystemen, um Klone aus der sekundären Tresorsicherung zu erstellen.</li> <li>• Erforderlich auf SnapMirror Zielsystemen, um Klone aus sekundären SnapMirror Backups zu erstellen.</li> </ul>                                                                                                                                                                                           |
| Protokolllizenzen                       | <ul style="list-style-type: none"> <li>• iSCSI- oder FC-Lizenz für LUNs</li> <li>• CIFS-Lizenz für SMB-Freigaben</li> <li>• NFS-Lizenz für VMDKs vom Typ NFS</li> <li>• iSCSI- oder FC-Lizenz für VMDKs vom Typ VMFS</li> </ul> <p>Erforderlich auf SnapMirror Zielsystemen, um Daten bereitzustellen, wenn kein Quellvolume verfügbar ist.</p>                                                                                                                                                                                                                                                  |
| SnapCenter Standard-Lizenzen (optional) | <p>Sekundärziele</p> <div>  <p>Es wird empfohlen, ist aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standard-Lizenzen auf sekundären Zielen nicht aktiviert sind, können Sie SnapCenter nach der Durchführung eines Failover-Vorgangs nicht zum Sichern von Ressourcen auf dem sekundären Ziel verwenden. Auf sekundären Zielen ist jedoch eine FlexClone -Lizenz erforderlich, um Klon- und Überprüfungsvorgänge durchzuführen.</p> </div> |

| Lizenz                                  | Wo erforderlich                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Single Mailbox Recovery (SMBR)-Lizenzen | <p>Wenn Sie das SnapCenter -Plug-in für Exchange zum Verwalten von Microsoft Exchange Server-Datenbanken und Single Mailbox Recovery (SMBR) verwenden, benötigen Sie eine zusätzliche Lizenz für SMBR, die je nach Benutzerpostfach separat erworben werden muss.</p> <p>Die Verfügbarkeit von NetApp® Single Mailbox Recovery (EOA) endet am 12. Mai 2023. Weitere Informationen finden Sie unter "<a href="#">CPC-00507</a>". NetApp wird Kunden, die Postfachkapazität, Wartung und Support über die am 24. Juni 2020 eingeführten Marketing-Teilenummern erworben haben, für die Dauer des Supportanspruchs weiterhin unterstützen.</p> <p>NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. Ontrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können neue Ontrack PowerControls-Softwarelizenzen sowie Wartungs- und Supportverlängerungen für Ontrack PowerControls von Ontrack (über <a href="mailto:licensingteam@ontrack.com">licensingteam@ontrack.com</a>) für eine detaillierte Postfachwiederherstellung nach dem EOA-Datum (12. Mai 2023) erwerben.</p> |



Die Lizenzen für SnapCenter Advanced und SnapCenter NAS File Services sind veraltet und nicht mehr verfügbar. Die Standardlizenz und die kapazitätsbasierte Lizenz sind für Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP und Azure NetApp Files nicht mehr erforderlich.

Sie sollten eine oder mehrere SnapCenter -Lizenzen installieren. Informationen zum Hinzufügen von Lizenzen finden Sie unter "[Hinzufügen von Controller-basierten Lizenzen für SnapCenter Standard](#)".

## SnapMirror Active Sync in SnapCenter

SnapMirror Active Sync ermöglicht die Weiterführung des Betriebs von Geschäftsdiensten auch bei einem vollständigen Site-Ausfall und unterstützt Anwendungen bei einem transparenten Failover mithilfe einer sekundären Kopie. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

Weitere Informationen zu SnapMirror Active Sync finden Sie unter "[SnapMirror Active Sync-Übersicht](#)".

Stellen Sie für die aktive Synchronisierung von SnapMirror sicher, dass Sie die verschiedenen Hardware-, Software- und Systemkonfigurationsanforderungen erfüllt haben. Weitere Informationen finden Sie unter "[Voraussetzungen](#)".

Die für diese Funktion unterstützten Plug-ins sind SnapCenter Plug-in für SQL Server, SnapCenter Plug-in für Windows, SnapCenter Plug-in für Oracle-Datenbanken, SnapCenter Plug-in für SAP HANA-Datenbanken,



Um die Host-Initiator-Nähe in SnapCenter zu unterstützen, sollte der Wert, entweder Quelle oder Ziel, in ONTAP festgelegt werden.

Die in SnapCenter nicht unterstützten Anwendungsfälle:

- Wenn Sie die vorhandenen asymmetrischen SnapMirror Active Sync-Workloads in symmetrische umwandeln, indem Sie die Richtlinie für die SnapMirror Active Sync-Beziehungen in ONTAP von *automatedfailover* in *automatedfailoverduplex* ändern, wird dies in SnapCenter nicht unterstützt.
- Wenn Sicherungen einer Ressourcengruppe vorhanden sind (bereits in SnapCenter geschützt) und dann die Speicherrichtlinie für die SnapMirror -Active-Sync-Beziehungen von *automatedfailover* in *automatedfailoverduplex* in ONTAP geändert wird, wird dies in SnapCenter nicht unterstützt.

## Schlüsselbegriffe des Datenschutzes

Machen Sie sich vor der Verwendung von SnapCenter mit den wichtigsten Konzepten für Sicherung, Klonen und Wiederherstellen vertraut.

### Ressourcen

Zu den Ressourcen gehören Datenbanken, Windows-Dateisysteme oder Dateifreigaben, die mit SnapCenter gesichert oder geklont wurden. Abhängig von Ihrer Umgebung können Ressourcen auch Datenbankinstanzen, SQL Server-Verfügbarkeitsgruppen, Oracle-Datenbanken, RAC-Datenbanken oder benutzerdefinierte Anwendungsgruppen sein.

### Ressourcengruppe

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster, möglicherweise von mehreren Hosts und Clustern. An einer Ressourcengruppe ausgeführte Vorgänge gelten für alle darin enthaltenen Ressourcen basierend auf dem angegebenen Zeitplan. Sie können On-Demand- oder geplante Backups für einzelne Ressourcen oder Gruppen durchführen.



Wenn ein Host in einer gemeinsam genutzten Ressourcengruppe in den Wartungsmodus wechselt, werden alle geplanten Vorgänge für diese Gruppe auf allen Hosts ausgesetzt.

Verwenden Sie relevante Plug-ins, um bestimmte Ressourcen zu sichern: Datenbank-Plug-ins für Datenbanken, Dateisystem-Plug-ins für Dateisysteme und das SnapCenter Plug-in for VMware vSphere für VMs und Datenspeicher.

### Richtlinien

Richtlinien legen die Sicherungshäufigkeit, die Aufbewahrung von Kopien, Replikation, Skripts und andere Merkmale von Datenschutzvorgängen fest.

Beim Erstellen einer Ressourcengruppe oder beim Durchführen einer On-Demand-Sicherung können eine oder mehrere Richtlinien ausgewählt werden.

Eine Ressourcengruppe definiert, was geschützt werden muss und wann es hinsichtlich Tag und Uhrzeit geschützt werden soll. Eine Richtlinie beschreibt, wie der Schutz umgesetzt wird. Wenn beispielsweise eine Sicherung aller Datenbanken oder Dateisysteme eines Hosts erforderlich ist, kann eine Ressourcengruppe erstellt werden, die alle Datenbanken oder Dateisysteme auf dem Host umfasst. Der Ressourcengruppe könnten dann zwei Richtlinien zugeordnet werden: eine Tagesrichtlinie und eine Stundenrichtlinie.

Beim Erstellen der Ressourcengruppe und Anhängen der Richtlinien ist es möglich, sie so zu konfigurieren, dass täglich eine vollständige Sicherung und stündlich ein weiterer Zeitplan für Protokollsicherungen durchgeführt wird.

Bei Datenschutzvorgängen können benutzerdefinierte Prescripts und Postscripts verwendet werden. Diese Skripte ermöglichen eine Automatisierung entweder vor oder nach dem Datenschutzjob. Beispielsweise könnte ein Skript automatisch über Fehler oder Warnungen bei Datenschutzaufträgen informieren. Bevor Sie Präskripte und Postskripte einrichten, ist es wichtig, die Anforderungen zum Erstellen dieser Skripte zu verstehen.

## Verwendung von Präskripten und Postskripten

Benutzerdefinierte Prescripts und Postscripts können Ihre Datenschutzaufgaben vor oder nach dem Job automatisieren. Sie können beispielsweise ein Skript hinzufügen, das Sie über Jobfehler oder Warnungen benachrichtigt. Stellen Sie vor der Einrichtung sicher, dass Sie die Anforderungen für diese Skripte verstehen.

### Unterstützte Skripttypen

Die folgenden Skripttypen werden für Windows unterstützt:

- Batchdateien
- PowerShell-Skripts
- Perl-Skripte

Für UNIX werden die folgenden Skripttypen unterstützt:

- Perl-Skripte
- Python-Skripte
- Shell-Skripte



Neben der Standard-Bash-Shell werden auch andere Shells wie SH-Shell, K-Shell und C-Shell unterstützt.

### Skriptpfad

Alle Prescripts und Postscripts, die als Teil von SnapCenter -Vorgängen auf nicht virtualisierten und virtualisierten Speichersystemen ausgeführt werden, werden auf dem Plug-In-Host ausgeführt.

- Die Windows-Skripte sollten sich auf dem Plug-In-Host befinden.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

- Die UNIX-Skripte sollten sich auf dem Plug-In-Host befinden.



Der Skriptpfad wird zum Zeitpunkt der Ausführung validiert.

### Wo Skripte angegeben werden

Skripte werden in Sicherungsrichtlinien angegeben. Wenn ein Sicherungsauftrag gestartet wird, verknüpft die Richtlinie das Skript automatisch mit den zu sichernden Ressourcen. Wenn Sie eine Sicherungsrichtlinie

erstellen, können Sie die Prescript- und Postscript-Argumente angeben.



Sie können nicht mehrere Skripte angeben.

### **Skript-Timeouts**

Das Timeout ist standardmäßig auf 60 Sekunden eingestellt. Sie können den Timeout-Wert ändern.

### **Skriptausgabe**

Das Standardverzeichnis für die Windows-Prescripts- und Postscripts-Ausgabedateien ist Windows\System32.

Es gibt keinen Standardspeicherort für die UNIX-Prescripts und Postscripts. Sie können die Ausgabedatei an einen beliebigen Speicherort umleiten.

## **Von SnapCenter unterstützte Speichersysteme und Anwendungen**

Sie sollten die von SnapCenter unterstützten Speichersysteme, Anwendungen und Datenbanken kennen.

### **Unterstützte Speichersysteme**

- NetApp ONTAP 9.12.1 und höher
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

Unterstützt Non-Volatile Memory Express (NVMe) über Transport Control Protocol (TCP).

Informationen zu Amazon FSx for NetApp ONTAP finden Sie unter "[Amazon FSx for NetApp ONTAP -Dokumentation](#)".

- NetApp ASA r2-Systeme, auf denen NetApp ONTAP 9.16.1 ausgeführt wird.

### **Unterstützte Anwendungen und Datenbanken**

SnapCenter unterstützt den Schutz verschiedener Anwendungen und Datenbanken. Ausführliche Informationen zu den unterstützten Anwendungen und Datenbanken finden Sie unter "[NetApp Interoperabilitätsmatrix-Tool](#)".

SnapCenter unterstützt den Schutz von Oracle- und Microsoft SQL-Workloads in VMware Cloud auf Amazon Web Services (AWS) Software-Defined Data Center (SDDC)-Umgebungen. "[Weitere Informationen](#)".

## **Authentifizierungsmethoden für SnapCenter -Anmeldeinformationen**

Für Anmeldeinformationen werden je nach Anwendung oder Umgebung unterschiedliche Authentifizierungsmethoden verwendet. Anmeldeinformationen authentifizieren Benutzer, damit sie SnapCenter -Vorgänge ausführen können. Sie sollten einen Satz Anmeldeinformationen für die Installation von Plug-Ins und einen anderen für Datenschutzvorgänge erstellen.

## **Windows-Authentifizierung**

Die Windows-Authentifizierungsmethode authentifiziert sich gegenüber Active Directory. Für die Windows-Authentifizierung wird Active Directory außerhalb von SnapCenter eingerichtet. SnapCenter authentifiziert ohne zusätzliche Konfiguration. Sie benötigen Windows-Anmeldeinformationen, um Hosts hinzuzufügen, Plug-In-Pakete zu installieren und Jobs zu planen.

## **Nicht vertrauenswürdige Domänenauthentifizierung**

SnapCenter ermöglicht Benutzern und Gruppen, die zu nicht vertrauenswürdigen Domänen gehören, das Erstellen von Windows-Anmeldeinformationen. Damit die Authentifizierung erfolgreich ist, sollten Sie die nicht vertrauenswürdigen Domänen bei SnapCenter registrieren.

## **Lokale Arbeitsgruppenauthentifizierung**

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen mit lokalen Arbeitsgruppenbenutzern und -gruppen. Die Windows-Authentifizierung für lokale Arbeitsgruppenbenutzer und -gruppen erfolgt nicht während der Erstellung der Windows-Anmeldeinformationen, sondern wird verschoben, bis die Hostregistrierung und andere Hostvorgänge durchgeführt werden.

## **SQL Server-Authentifizierung**

Die SQL-Authentifizierungsmethode authentifiziert sich gegenüber einer SQL Server-Instanz. Dies bedeutet, dass in SnapCenter eine SQL Server-Instanz erkannt werden muss. Daher müssen Sie vor dem Hinzufügen von SQL-Anmeldeinformationen einen Host hinzufügen, Plug-In-Pakete installieren und Ressourcen aktualisieren. Sie benötigen eine SQL Server-Authentifizierung, um Vorgänge wie die Planung auf SQL Server oder die Ermittlung von Ressourcen durchzuführen.

## **Linux-Authentifizierung**

Die Linux-Authentifizierungsmethode authentifiziert sich gegenüber einem Linux-Host. Sie benötigen eine Linux-Authentifizierung während des ersten Schritts, bei dem Sie den Linux-Host hinzufügen und das SnapCenter Plug-Ins-Paket für Linux remote über die SnapCenter -GUI installieren.

## **AIX-Authentifizierung**

Die AIX-Authentifizierungsmethode authentifiziert gegenüber einem AIX-Host. Sie benötigen eine AIX-Authentifizierung während des ersten Schritts, bei dem Sie den AIX-Host hinzufügen und das SnapCenter Plug-Ins-Paket für AIX remote über die SnapCenter -GUI installieren.

## **Oracle-Datenbankauthentifizierung**

Die Oracle-Datenbankauthentifizierungsmethode authentifiziert gegenüber einer Oracle-Datenbank. Sie benötigen eine Oracle-Datenbankauthentifizierung, um Vorgänge an der Oracle-Datenbank auszuführen, wenn die Betriebssystemauthentifizierung (OS) auf dem Datenbankhost deaktiviert ist. Bevor Sie Anmeldeinformationen für eine Oracle-Datenbank hinzufügen, sollten Sie daher einen Oracle-Benutzer mit Sysdba-Berechtigungen in der Oracle-Datenbank erstellen.

## **Oracle ASM-Authentifizierung**

Die Oracle ASM-Authentifizierungsmethode authentifiziert sich gegenüber einer Oracle Automatic Storage Management (ASM)-Instanz. Die Oracle ASM-Authentifizierung ist erforderlich, wenn Sie auf eine Oracle ASM-Instanz zugreifen müssen und die Betriebssystemauthentifizierung auf dem Datenbankhost deaktiviert ist. Erstellen Sie vor dem Hinzufügen einer Oracle ASM-Anmeldeinformation einen Oracle-Benutzer mit

Systemberechtigungen in der ASM-Instanz.

## **RMAN-Katalogauthentifizierung**

Die RMAN-Katalogauthentifizierungsmethode authentifiziert sich gegenüber der Oracle Recovery Manager (RMAN)-Katalogdatenbank. Wenn Sie einen externen Katalogmechanismus konfiguriert und Ihre Datenbank bei der Katalogdatenbank registriert haben, müssen Sie die RMAN-Katalogauthentifizierung hinzufügen.

## **Unterstützte SnapCenter -Vorgänge für ASA r2-Systeme**

ASA r2-Speichersysteme werden ab SnapCenter 6.1 unterstützt. ["Erfahren Sie mehr über ASA r2-Systeme"](#)

SnapCenter nutzt REST-APIs, um alle Vorgänge auf ASA r2-Systemen auszuführen, die ZAPIs nicht unterstützen.

### **Von SnapCenter für ASA r2-Systeme unterstützte Vorgänge**

- Erstellen primärer Backups von Anwendungen über VMDK
- Übertragen von Konsistenzgruppen-Snapshots auf ein sekundäres Speichersystem
- Wiederherstellen der Backups von primären und sekundären Speichersystemen auf dem ursprünglichen Host oder dem alternativen Host
  - In-Place-Wiederherstellung von primären und sekundären Speichersystemen mit VMware vMotion
  - Verbinden und Kopieren und Wiederherstellen von primären und sekundären Speichersystemen
- Klonen der Backups auf den ursprünglichen Host oder auf den alternativen Host

SnapCenter kann ONTAP Konsistenzgruppen erkennen oder erstellen. Es kann außerdem SnapMirror -Beziehungen zum Zielcluster für sekundären Schutz bereitstellen und initialisieren.

Informationen zum Aktivieren des sekundären Schutzes auf ASA R2-Systemen für Ihre Anwendung finden Sie unter:

- ["Aktivieren Sie den sekundären Schutz für Microsoft SQL Server-Ressourcen"](#)
- ["Aktivieren Sie den sekundären Schutz für SAP HANA-Ressourcen"](#)
- ["Aktivieren Sie den sekundären Schutz für Oracle-Ressourcen"](#)
- ["Aktivieren Sie den sekundären Schutz für Windows-Dateisysteme"](#)
- ["Aktivieren Sie den sekundären Schutz für IBM Db2-Ressourcen"](#)
- ["Aktivieren Sie den sekundären Schutz für PostgreSQL-Ressourcen"](#)
- ["Aktivieren Sie den sekundären Schutz für MySQL-Ressourcen"](#)
- ["Aktivieren Sie den sekundären Schutz für Unix-Dateisysteme"](#)

### **Vorgänge, die von SnapCenter für ASA r2-Systeme nicht unterstützt werden**

- Raw Device Mapping (RDM)
- Anwendungsvolumes für Oracle
- SAP HANA NDV
- LockVault



- Manipulationssichere Schnappschüsse
- FlexGroup -Volumina
- Hierarchische Konsistenzgruppe
- Migration von ASA, AFF oder FAS Speichersystemen zu ASA r2-Speichersystemen
- Schutz von Datenbanken mit einer Mischung aus ASA, AFF oder FAS -Ressourcen und ASA r2-Ressourcen
- Umbenennen von Snapshots
- Sekundäre Bereitstellung des Protokollverzeichnisses des SQL-Plugin-Hosts

## Schnellstart für die SnapCenter software

Die Kurzanleitung beschreibt die grundlegenden Schritte zur Installation und Konfiguration der SnapCenter software.

**1**

### Vorbereiten der Installation von SnapCenter Server

Sie sollten sicherstellen, dass alle Anforderungen zur Installation des SnapCenter -Servers erfüllt sind.

- ["Anforderungen"](#)
- ["Registrieren Sie sich, um auf die SnapCenter software zuzugreifen"](#)
- ["Aktivieren Sie die Multifaktor-Authentifizierung"](#)

**2**

### Installieren Sie SnapCenter Server

Der SnapCenter -Server kann entweder auf Windows- oder Linux-Hosts installiert werden. Laden Sie das SnapCenter Server-Installationspaket von der ["NetApp Support Site"](#) und führen Sie das Installationsprogramm aus.

- ["Installieren Sie den SnapCenter -Server unter Windows"](#)
- ["Installieren Sie SnapCenter Server unter Linux"](#)

**3**

### SnapCenter Server konfigurieren

Nach der Installation des SnapCenter -Servers sollten Sie ihn entsprechend Ihrer Umgebung konfigurieren.

**4**

### Installieren Sie das Plug-In für Ihre Anwendung

Stellen Sie sicher, dass alle Voraussetzungen für die Installation des anwendungsspezifischen Plug-ins je nach verwendeter Anwendung erfüllt sind, und fahren Sie dann mit der Installation des jeweiligen Plug-ins fort.

**5**

### Schützen Sie Ihre Anwendung

Nach der erfolgreichen Installation des SnapCenter -Servers und der erforderlichen Plug-Ins können Sie mit der Erstellung von Anwendungssicherungen beginnen. Diese Backups können später bei Bedarf zur Wiederherstellung und zum Klonen verwendet werden.

# Installieren und Konfigurieren von SnapCenter Server

## Vorbereiten der Installation des SnapCenter -Servers

### Voraussetzungen für die Installation von SnapCenter Server

Bevor Sie SnapCenter Server auf einem Windows- oder Linux-Host installieren, sollten Sie überprüfen und sicherstellen, dass alle Anforderungen für Ihre Umgebung erfüllt sind.

#### Domänen- und Arbeitsgruppenanforderungen für Windows-Host

Der SnapCenter -Server kann auf einem Windows-Host installiert werden, der sich entweder in einer Domäne oder in einer Arbeitsgruppe befindet.

Der Benutzer mit Administratorrechten darf den SnapCenter -Server installieren.

- Active Directory-Domäne: Sie müssen einen Domänenbenutzer mit lokalen Administratorrechten verwenden. Der Domänenbenutzer muss Mitglied der lokalen Administratorgruppe auf dem Windows-Host sein.
- Arbeitsgruppen: Sie müssen ein lokales Konto mit lokalen Administratorrechten verwenden.

Während Domänenvertrauensstellungen, Mehrodomänengesamtstrukturen und domänenübergreifende Vertrauensstellungen unterstützt werden, werden gesamtstrukturübergreifende Domänen nicht unterstützt. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu Active Directory-Domänen und -Vertrauensstellungen.



Nach der Installation des SnapCenter -Servers sollten Sie die Domäne, in der sich der SnapCenter Host befindet, nicht ändern. Wenn Sie den SnapCenter Server-Host aus der Domäne entfernen, in der er sich bei der Installation des SnapCenter Servers befand, und dann versuchen, den SnapCenter Server zu deinstallieren, schlägt der Deinstallationsvorgang fehl.

### Platz- und Größenanforderungen

Sie sollten mit den Platz- und Größenanforderungen vertraut sein.

| Artikel                                                                            | Windows-Hostanforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Linux-Hostanforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                    | <p>Microsoft Windows</p> <p>Es werden nur die Betriebssystemversionen Englisch, Deutsch, Japanisch und vereinfachtes Chinesisch unterstützt.</p> <p>Aktuelle Informationen zu unterstützten Versionen finden Sie unter <a href="https://imt.netapp.com/matrix/imt.jsp?components=121033;&amp;solution=1258&amp;isHWU&amp;src=IMT[\" interoperabilitätsmatrix-tool\"]"="" netapp="">https://imt.netapp.com/matrix/imt.jsp?components=121033;&amp;solution=1258&amp;isHWU&amp;src=IMT[\"NetApp Interoperabilitätsmatrix-Tool\"]</a>.</p> | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux (RHEL) 8 und 9</li> <li>• SUSE Linux Enterprise Server (SLES) 15</li> </ul> <p>Aktuelle Informationen zu unterstützten Versionen finden Sie unter <a href="https://imt.netapp.com/matrix/imt.jsp?components=121032;&amp;solution=1258&amp;isHWU&amp;src=IMT[\" interoperabilitätsmatrix-tool\"]"="" netapp="">https://imt.netapp.com/matrix/imt.jsp?components=121032;&amp;solution=1258&amp;isHWU&amp;src=IMT[\"NetApp Interoperabilitätsmatrix-Tool\"]</a>.</p> |
| Minimale CPU-Anzahl                                                                | 4 Kerne                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 4 Kerne                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Mindest-RAM                                                                        | <p>8 GB</p> <div>  <p>Der Pufferpool des MySQL-Servers verwendet 20 Prozent des gesamten RAM.</p> </div>                                                                                                                                                                                                                                                                                                                                              | 8 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Mindestfestplattenspeicherplatz für die SnapCenter Server-Software und -Protokolle | <p>7 GB</p> <div>  <p>Wenn sich das SnapCenter Repository auf demselben Laufwerk befindet, auf dem SnapCenter Server installiert ist, werden 15 GB empfohlen.</p> </div>                                                                                                                                                                                                                                                                            | 15 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Mindestfestplattenspeicherplatz für das SnapCenter -Repository                     | <p>8 GB</p> <div>  <p>HINWEIS: Wenn sich der SnapCenter -Server auf demselben Laufwerk befindet, auf dem das SnapCenter Repository installiert ist, werden 15 GB empfohlen.</p> </div>                                                                                                                                                                                                                                                              | Nicht zutreffend                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Artikel                      | Windows-Hostanforderungen                                                                                                                                                   | Linux-Hostanforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Erforderliche Softwarepakete | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell 7.4.2 oder höher</li> </ul> | <ul style="list-style-type: none"> <li>• .NET Framework 8.0.12 (und alle nachfolgenden 8.0.x-Patches)</li> <li>• PowerShell 7.4.2 oder höher</li> <li>• Nginx ist ein Webserver, der als Reverse-Proxy verwendet werden kann</li> <li>• Pam-devel</li> </ul> <p>PAM (Pluggable Authentication Modules) ist ein Systemsicherheitstool, mit dem Systemadministratoren Authentifizierungsrichtlinien festlegen können, ohne Programme, die die Authentifizierung durchführen, neu kompilieren zu müssen.</p> |



ASP.NET Core benötigt IIS\_IUSRS, um auf das temporäre Dateisystem im SnapCenter Server unter Windows zuzugreifen.

## SAN-Hostanforderungen

SnapCenter enthält keine Host-Dienstprogramme oder ein DSM. Wenn der SnapCenter Host Teil einer SAN-Umgebung (FC/iSCSI) ist, müssen Sie möglicherweise zusätzliche Software auf dem SnapCenter -Server -Host installieren und konfigurieren.

- Host-Dienstprogramme: Die Host-Dienstprogramme unterstützen FC und iSCSI und ermöglichen Ihnen die Verwendung von MPIO auf Ihren Windows-Servern. "[Weitere Informationen](#)".
- Microsoft DSM für Windows MPIO: Diese Software arbeitet mit Windows MPIO-Treibern, um mehrere Pfade zwischen NetApp und Windows-Hostcomputern zu verwalten. Für Hochverfügbarkeitskonfigurationen ist ein DSM erforderlich.



Wenn Sie ONTAP DSM verwendet haben, sollten Sie zu Microsoft DSM migrieren. Weitere Informationen finden Sie unter "[So migrieren Sie von ONTAP DSM zu Microsoft DSM](#)".

## Browseranforderungen

Die SnapCenter software unterstützt Chrome 125 und höher sowie Microsoft Edge 110.0.1587.17 und höher.

## Portanforderungen

Die SnapCenter software benötigt unterschiedliche Ports für die Kommunikation zwischen verschiedenen Komponenten.

- Anwendungen können keinen Port gemeinsam nutzen.

- Für anpassbare Ports können Sie während der Installation einen benutzerdefinierten Port auswählen, wenn Sie den Standardport nicht verwenden möchten.
- Bei festen Ports sollten Sie die Standard-Portnummer akzeptieren.
- Firewalls
  - Firewalls, Proxys oder andere Netzwerkgeräte sollten die Verbindungen nicht stören.
  - Wenn Sie bei der Installation von SnapCenter einen benutzerdefinierten Port angeben, sollten Sie für den SnapCenter Plug-in Loader eine Firewall-Regel auf dem Plug-in-Host für diesen Port hinzufügen.

In der folgenden Tabelle sind die verschiedenen Ports und ihre Standardwerte aufgeführt.

| Portname                                    | Portnummern | Protokoll | Richtung      | Beschreibung                                                                                                                                                                                                                                                                        |
|---------------------------------------------|-------------|-----------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter<br>-Anschluss                    | 8146        | HTTPS     | Bidirektional | <p>Dieser Port wird für die Kommunikation zwischen dem SnapCenter Client (dem SnapCenter -Benutzer) und dem SnapCenter -Server verwendet und wird auch für die Kommunikation von den Plug-In-Hosts zum SnapCenter -Server verwendet.</p> <p>Sie können die Portnummer anpassen.</p> |
| SnapCenter<br>SMCore-<br>Kommunikationsport | 8145        | HTTPS     | Bidirektional | <p>Dieser Port wird für die Kommunikation zwischen dem SnapCenter Server und den Hosts verwendet, auf denen die SnapCenter Plug-Ins installiert sind.</p> <p>Sie können die Portnummer anpassen.</p>                                                                                |

| Portname             | Portnummern | Protokoll | Richtung | Beschreibung                                                                                                                                                                                                        |
|----------------------|-------------|-----------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scheduler-Dienstport | 8154        | HTTPS     |          | <p>Dieser Port wird verwendet, um die SnapCenter -Scheduler -Workflows für alle verwalteten Plug-Ins innerhalb des SnapCenter -Serverhosts zentral zu orchestrieren.</p> <p>Sie können die Portnummer anpassen.</p> |
| RabbitMQ-Port        | 5672        | TCP       |          | <p>Dies ist der Standardport, auf dem RabbitMQ lauscht, und er wird für die Publisher-Subscriber-Modellkommunikation zwischen dem Scheduler-Dienst und SnapCenter verwendet.</p>                                    |
| MySQL-Port           | 3306        | HTTPS     |          | <p>Der Port wird für die Kommunikation mit der SnapCenter -Repository -Datenbank verwendet. Sie können sichere Verbindungen vom SnapCenter -Server zum MySQL-Server erstellen. <a href="#">"Mehr erfahren"</a></p>  |

| Portname                                             | Portnummern | Protokoll | Richtung       | Beschreibung                                                                                                                                                                                                                                |
|------------------------------------------------------|-------------|-----------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows-Plug-In-Hosts                                | 135, 445    | TCP       |                | Dieser Port wird für die Kommunikation zwischen dem SnapCenter -Server und dem Host verwendet, auf dem das Plug-In installiert wird. Der zusätzliche dynamische Portbereich, der von Microsoft angegeben wird, sollte ebenfalls offen sein. |
| Linux- oder AIX-Plug-in-Hosts                        | 22          | SSH       | Unidirektional | Dieser Port wird für die Kommunikation zwischen dem SnapCenter -Server und dem Host verwendet und vom Server zum Client-Host initiiert.                                                                                                     |
| SnapCenter Plug-In-Paket für Windows, Linux oder AIX | 8145        | HTTPS     | Bidirektional  | Dieser Port wird für die Kommunikation zwischen SMCore und Hosts verwendet, auf denen das Plug-In-Paket installiert ist. Anpassbar.<br><br>Sie können die Portnummer anpassen.                                                              |
| SnapCenter -Plug-in für Oracle-Datenbank             | 27216       |           |                | Der Standard-JDBC-Port wird vom Plug-In für Oracle zum Herstellen einer Verbindung mit der Oracle-Datenbank verwendet.                                                                                                                      |

| Portname                                        | Portnummern                                                                          | Protokoll                                                                 | Richtung      | Beschreibung                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter -Plug-in für Exchange-Datenbank      | 909                                                                                  |                                                                           |               | Der Standard-NET.TCP-Port wird vom Plug-In für Windows zum Herstellen einer Verbindung mit den Exchange-VSS-Rückrufen verwendet.                                                                                                                                                                                    |
| Von NetApp unterstützte Plug-ins für SnapCenter | 9090                                                                                 | HTTPS                                                                     |               | <p>Dies ist ein interner Port, der nur auf dem Plug-In-Host verwendet wird. Es ist keine Firewall-Ausnahme erforderlich.</p> <p>Die Kommunikation zwischen dem SnapCenter -Server und den Plug-Ins wird über Port 8145 geleitet.</p>                                                                                |
| ONTAP Cluster oder SVM-Kommunikationsport       | <ul style="list-style-type: none"> <li>• 443 (HTTPS)</li> <li>• 80 (HTTP)</li> </ul> | <ul style="list-style-type: none"> <li>• HTTPS</li> <li>• HTTP</li> </ul> | Bidirektional | Der Port wird vom SAL (Storage Abstraction Layer) für die Kommunikation zwischen dem Host, auf dem SnapCenter Server ausgeführt wird, und SVM verwendet. Der Port wird derzeit auch vom SAL auf SnapCenter für Windows-Plug-in-Hosts für die Kommunikation zwischen dem SnapCenter -Plug-in-Host und SVM verwendet. |



| Portname                                  | Portnummern                                                                                          | Protokoll                                                                 | Richtung      | Beschreibung                                                                                                                                                                                           |
|-------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter Plug-in für SAP HANA-Datenbank | <ul style="list-style-type: none"> <li>• 3instance_number13</li> <li>• 3instance_number15</li> </ul> | <ul style="list-style-type: none"> <li>• HTTPS</li> <li>• HTTP</li> </ul> | Bidirektional | <p>Bei einem Multitenant-Datenbankcontainer (MDC) mit einem einzelnen Mandanten endet die Portnummer mit 13; bei Nicht-MDC endet die Portnummer mit 15.</p> <p>Sie können die Portnummer anpassen.</p> |
| SnapCenter Plug-in für PostgreSQL         | 5432                                                                                                 |                                                                           |               | <p>Dieser Port ist der PostgreSQL-Standardport, der vom Plug-In für PostgreSQL für die Kommunikation mit dem PostgreSQL-Cluster verwendet wird.</p> <p>Sie können die Portnummer anpassen.</p>         |

## Registrieren Sie sich, um auf die SnapCenter software zuzugreifen

Sie sollten sich für den Zugriff auf die SnapCenter software registrieren, wenn Sie neu bei Amazon FSx for NetApp ONTAP oder Azure NetApp Files sind und kein bestehendes NetApp Konto haben.

### Bevor Sie beginnen

- Sie sollten Zugriff auf die Unternehmens-E-Mail-ID haben.
- Wenn Sie Azure NetApp Files verwenden, sollten Sie über die Azure-Abonnement-ID verfügen.
- Wenn Sie Amazon FSx for NetApp ONTAP verwenden, sollten Sie die Dateisystem-ID Ihres FSx für ONTAP -Dateisystems haben.

### Informationen zu diesem Vorgang

Ihre Registrierung unterliegt der Validierung Ihrer Informationen und es kann bis zu einem Tag dauern, bis das neue NetApp Support Site (NSS)-Konto bestätigt und vom **Gast-Zugriff** auf **vollständigen** Zugriff aktualisiert wird.

### Schritte

1. Klicken <https://mysupport.netapp.com/site/user/registration> zur Registrierung.

2. Geben Sie Ihre Unternehmens-E-Mail-ID ein, füllen Sie das Captcha aus, akzeptieren Sie die Datenschutzrichtlinie von NetApp und klicken Sie auf **Senden**.
3. Authentifizieren Sie die Registrierung, indem Sie das an Ihre E-Mail-ID gesendete OTP eingeben und auf **Weiter** klicken.
4. Geben Sie auf der Seite zum Abschluss der Registrierung die folgenden Details ein, um die Registrierung abzuschließen.
  - a. Wählen Sie \* NetApp -Kunde/Endbenutzer\*.
  - b. Geben Sie im Feld SERIENNUMMER entweder die Azure-Abonnement-ID ein, wenn Sie Azure NetApp Files verwenden, oder die Dateisystem-ID, wenn Sie Amazon FSx for NetApp ONTAP verwenden.



Sie können ein Ticket erstellen unter <https://mysupport.netapp.com/site/help> wenn Sie während der Registrierung auf ein Problem stoßen oder den Status erfahren möchten.

## Multi-Faktor-Authentifizierung (MFA)

### Verwalten der Multi-Faktor-Authentifizierung (MFA)

Sie können die Multi-Faktor-Authentifizierungsfunktion (MFA) im Active Directory Federation Service (AD FS)-Server und im SnapCenter Server verwalten.

#### Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA).

Sie können die MFA-Funktionalität für SnapCenter Server mithilfe von PowerShell-Befehlen aktivieren.

#### Informationen zu diesem Vorgang

- SnapCenter unterstützt SSO-basierte Anmeldungen, wenn andere Anwendungen im selben AD FS konfiguriert sind. In bestimmten AD FS-Konfigurationen erfordert SnapCenter möglicherweise aus Sicherheitsgründen eine Benutzerauthentifizierung, abhängig von der Persistenz der AD FS-Sitzung.
- Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von `Get-Help command_name`. Alternativ können Sie auch sehen "[Referenzhandbuch für SnapCenter -Software-Cmdlets](#)".

#### Bevor Sie beginnen

- Der Windows Active Directory Federation Service (AD FS) sollte in der jeweiligen Domäne aktiv und betriebsbereit sein.
- Sie sollten über einen von AD FS unterstützten Multi-Faktor-Authentifizierungsdienst wie Azure MFA, Cisco Duo usw. verfügen.
- Der Zeitstempel des SnapCenter und AD FS-Servers sollte unabhängig von der Zeitzone identisch sein.
- Beschaffen und konfigurieren Sie das autorisierte CA-Zertifikat für SnapCenter Server.

Ein CA-Zertifikat ist aus folgenden Gründen obligatorisch:

- Stellt sicher, dass die ADFS-F5-Kommunikation nicht unterbrochen wird, da die selbstsignierten Zertifikate auf Knotenebene eindeutig sind.
- Stellt sicher, dass während eines Upgrades, einer Reparatur oder einer Notfallwiederherstellung (DR) in einer eigenständigen oder Hochverfügbarkeitskonfiguration das selbstsignierte Zertifikat nicht neu erstellt wird, wodurch eine MFA-Neukonfiguration vermieden wird.

- Stellt IP-FQDN-Auflösungen sicher.

Informationen zum CA-Zertifikat finden Sie unter "[CA-Zertifikat-CSR-Datei generieren](#)".

## Schritte

1. Stellen Sie eine Verbindung zum Active Directory Federation Services (AD FS)-Host her.
2. Laden Sie die AD FS-Verbundmetadatendatei herunter von "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>".
3. Kopieren Sie die heruntergeladene Datei auf den SnapCenter -Server, um die MFA-Funktion zu aktivieren.
4. Melden Sie sich über PowerShell als SnapCenter -Administratorbenutzer beim SnapCenter -Server an.
5. Generieren Sie mithilfe der PowerShell-Sitzung die SnapCenter MFA-Metadatendatei mit dem Cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

Der Pfadparameter gibt den Pfad zum Speichern der MFA-Metadatendatei im SnapCenter Server-Host an.

6. Kopieren Sie die generierte Datei auf den AD FS-Host, um SnapCenter als Cliententität zu konfigurieren.
7. Aktivieren Sie MFA für SnapCenter Server mithilfe des *Set-SmMultiFactorAuthentication* Cmdlet.
8. (Optional) Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe von *Get-SmMultiFactorAuthentication* Cmdlet.
9. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf **Datei > Snap-In hinzufügen/entfernen**.
  - b. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
  - c. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
  - d. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Persönlich > Zertifikate**.
  - e. Klicken Sie mit der rechten Maustaste auf das an SnapCenter gebundene CA-Zertifikat und wählen Sie dann **Alle Aufgaben > Private Schlüssel verwalten**.
  - f. Führen Sie im Berechtigungsassistenten die folgenden Schritte aus:
    - i. Klicken Sie auf **Hinzufügen**.
    - ii. Klicken Sie auf **Standorte** und wählen Sie den betreffenden Host (oben in der Hierarchie) aus.
    - iii. Klicken Sie im Popup-Fenster **Standorte** auf **OK**.
    - iv. Geben Sie im Feld „Objektnamen“ „IIS\_IUSRS“ ein, klicken Sie auf **Namen überprüfen** und dann auf **OK**.

Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.

10. Öffnen Sie im AD FS-Host den AD FS-Verwaltungsassistenten und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie mit der rechten Maustaste auf **Vertrauensstellungen der vertrauenden Partei > Vertrauensstellung der vertrauenden Partei hinzufügen > Start**.
  - b. Wählen Sie die zweite Option, durchsuchen Sie die SnapCenter MFA-Metadatendatei und klicken Sie auf **Weiter**.
  - c. Geben Sie einen Anzeigenamen an und klicken Sie auf **Weiter**.
  - d. Wählen Sie nach Bedarf eine Zugriffskontrollrichtlinie aus und klicken Sie auf **Weiter**.

- e. Wählen Sie im nächsten Reiter die Standardeinstellungen aus.
- f. Klicken Sie auf **Fertig**.

SnapCenter wird jetzt mit dem angegebenen Anzeigenamen als vertrauende Partei angezeigt.

11. Wählen Sie den Namen aus und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf **Richtlinie zur Anspruchsausstellung bearbeiten**.
  - b. Klicken Sie auf **Regel hinzufügen** und dann auf **Weiter**.
  - c. Geben Sie einen Namen für die Anspruchsregel an.
  - d. Wählen Sie **Active Directory** als Attributspeicher aus.
  - e. Wählen Sie das Attribut als **User-Principal-Name** und den ausgehenden Anspruchstyp als **Name-ID**.
  - f. Klicken Sie auf **Fertig**.
12. Führen Sie die folgenden PowerShell-Befehle auf dem ADFS-Server aus.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-EncryptionCertificateRevocationCheck None
```

13. Führen Sie die folgenden Schritte aus, um zu bestätigen, dass die Metadaten erfolgreich importiert wurden.
  - a. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite und wählen Sie **Eigenschaften**.
  - b. Stellen Sie sicher, dass die Felder „Endpunkte“, „Kennungen“ und „Signatur“ ausgefüllt sind.
14. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

Die SnapCenter MFA-Funktionalität kann auch mithilfe von REST-APIs aktiviert werden.

Informationen zur Fehlerbehebung finden Sie unter "[Gleichzeitige Anmeldeversuche in mehreren Registerkarten zeigen einen MFA-Fehler](#)".

#### Aktualisieren der AD FS MFA-Metadaten

Sie sollten die AD FS MFA-Metadaten in SnapCenter aktualisieren, wenn es Änderungen am AD FS-Server gibt, z. B. Upgrade, Erneuerung des CA-Zertifikats, DR usw.

#### Schritte

1. Laden Sie die AD FS-Verbundmetadatendatei herunter von "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. Kopieren Sie die heruntergeladene Datei auf den SnapCenter -Server, um die MFA-Konfiguration zu aktualisieren.
3. Aktualisieren Sie die AD FS-Metadaten in SnapCenter, indem Sie das folgende Cmdlet ausführen:

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

## Aktualisieren Sie die SnapCenter MFA-Metadaten

Sie sollten die SnapCenter MFA-Metadaten in AD FS aktualisieren, wenn am ADFS-Server Änderungen vorgenommen werden, z. B. Reparaturen, Erneuerung des CA-Zertifikats, DR usw.

### Schritte

1. Öffnen Sie im AD FS-Host den AD FS-Verwaltungsassistenten und führen Sie die folgenden Schritte aus:

- a. Wählen Sie **Vertrauensstellungen der vertrauenden Partei** aus.
- b. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Partei, die für SnapCenter erstellt wurde, und wählen Sie **Löschen**.

Der benutzerdefinierte Name des Relying Party Trust wird angezeigt.

- c. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA).

Sehen ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#) .

2. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

## Deaktivieren Sie die Multi-Faktor-Authentifizierung (MFA).

### Schritte

1. Deaktivieren Sie MFA und bereinigen Sie die Konfigurationsdateien, die beim Aktivieren von MFA erstellt wurden, mithilfe des `Set-SmMultiFactorAuthentication` Cmdlet.
2. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

## Verwalten Sie die Multi-Faktor-Authentifizierung (MFA) mit Rest API, PowerShell und SCCLI

Die MFA-Anmeldung wird über Browser, REST-API, PowerShell und SCCLI unterstützt. MFA wird durch einen AD FS-Identitätsmanager unterstützt. Sie können MFA aktivieren, deaktivieren und MFA über GUI, REST-API, PowerShell und SCCLI konfigurieren.

### AD FS als OAuth/OIDC einrichten

#### AD FS mit dem Windows-GUI-Assistenten konfigurieren

1. Navigieren Sie zu **Server Manager Dashboard > Tools > ADFS-Verwaltung**.
2. Navigieren Sie zu **ADFS > Anwendungsgruppen**.
  - a. Klicken Sie mit der rechten Maustaste auf **Anwendungsgruppen**.
  - b. Wählen Sie **Anwendungsgruppe hinzufügen** und geben Sie **Anwendungsname** ein.
  - c. Wählen Sie **Serveranwendung**.
  - d. Klicken Sie auf **Weiter**.
3. Kopieren Sie **Client-ID**.

Dies ist die Client-ID. .. Fügen Sie der Umleitungs-URL eine Rückruf-URL (SnapCenter -Server-URL) hinzu. .. Klicken Sie auf **Weiter**.

4. Wählen Sie **Gemeinsames Geheimnis generieren**.

Kopieren Sie den geheimen Wert. Dies ist das Geheimnis des Kunden. .. Klicken Sie auf **Weiter**.

5. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.
  - a. Klicken Sie auf der Seite **Abgeschlossen** auf **Schließen**.
6. Klicken Sie mit der rechten Maustaste auf die neu hinzugefügte **Anwendungsgruppe** und wählen Sie **Eigenschaften**.
7. Wählen Sie in den App-Eigenschaften **Anwendung hinzufügen** aus.
8. Klicken Sie auf **Anwendung hinzufügen**.

Wählen Sie Web-API und klicken Sie auf **Weiter**.

9. Geben Sie auf der Seite „Web-API konfigurieren“ die im vorherigen Schritt erstellte SnapCenter -Server -URL und Client-ID in den Abschnitt „ID“ ein.
  - a. Klicken Sie auf **Hinzufügen**.
  - b. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite **Zugriffskontrollrichtlinie auswählen** die Kontrollrichtlinie entsprechend Ihren Anforderungen aus (z. B. „Jeden zulassen“ und „MFA erforderlich“) und klicken Sie auf **Weiter**.
11. Klicken Sie auf der Seite **Anwendungsberechtigung konfigurieren** standardmäßig auf „openid“ als Bereich. Klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

Klicken Sie auf der Seite **Abgeschlossen** auf **Schließen**.

13. Klicken Sie auf der Seite **Beispielanwendungseigenschaften** auf **OK**.
14. Von einem Autorisierungsserver (AD FS) ausgestelltes und von der Ressource zu verwendendes JWT-Token.

Der „aud“- oder Zielgruppenanspruch dieses Tokens muss mit der Kennung der Ressource oder Web-API übereinstimmen.

15. Bearbeiten Sie die ausgewählte WebAPI und überprüfen Sie, ob die Rückruf-URL (SnapCenter -Server -URL) und die Client-ID korrekt hinzugefügt wurden.

Konfigurieren Sie OpenID Connect, um einen Benutzernamen als Ansprüche bereitzustellen.

16. Öffnen Sie das Tool **AD FS-Verwaltung**, das sich im Menü **Tools** oben rechts im Server-Manager befindet.
  - a. Wählen Sie in der linken Seitenleiste den Ordner **Anwendungsgruppen** aus.
  - b. Wählen Sie die Web-API aus und klicken Sie auf **BEARBEITEN**.
  - c. Zur Registerkarte „Ausgabetransformationsregeln“
17. Klicken Sie auf **Regel hinzufügen**.
  - a. Wählen Sie im Dropdownmenü „Anspruchsregelvorlage“ die Option „LDAP-Attribute als Ansprüche senden“ aus.
  - b. Klicken Sie auf **Weiter**.
18. Geben Sie den Namen der **Anspruchsregel** ein.
  - a. Wählen Sie im Dropdown-Menü „Attributspeicher“ **Active Directory** aus.
  - b. Wählen Sie **User-Principal-Name** im Dropdown-Menü **LDAP-Attribut** und **UPN** im Dropdown-Menü

## Ausgehender Anspruchstyp.

c. Klicken Sie auf **Fertig**.

### Erstellen einer Anwendungsgruppe mit PowerShell-Befehlen

Sie können die Anwendungsgruppe und die Web-API erstellen und den Bereich und die Ansprüche mithilfe von PowerShell-Befehlen hinzufügen. Diese Befehle sind im automatisierten Skriptformat verfügbar. Weitere Informationen finden Sie unter <Link zum KB-Artikel>.

1. Erstellen Sie die neue Anwendungsgruppe in AD FS mit dem folgenden Befehl.

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier  
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier`Name Ihrer Anwendungsgruppe

`redirectURL`gültige URL zur Weiterleitung nach Autorisierung

2. Erstellen Sie die AD FS-Serveranwendung und generieren Sie das Clientgeheimnis.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"  
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL  
-Identifier $identifier -GenerateClientSecret
```

3. Erstellen Sie die ADFS-Web-API-Anwendung und konfigurieren Sie den Richtliniennamen, den sie verwenden soll.

```
$identifier = (New-Guid).Guid
```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier  
-Name "App Web API"
```

```
-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. Holen Sie sich die Client-ID und das Client-Geheimnis aus der Ausgabe der folgenden Befehle, da diese nur einmal angezeigt werden.

```
"client_id = $identifier"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. Erteilen Sie der AD FS-Anwendung die Berechtigungen „allatclaims“ und „openid“.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier  
-ServerRoleIdentifier $identifier -ScopeNames @('openid')
```

```
$transformrule = @"
```

```
@RuleTemplate = "LdapClaims"
```

```
@RuleName = "AD User properties and Groups"
```

```
c:[Type ==
```

```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

## 6. Schreiben Sie die Datei mit den Transformationsregeln.

```
$transformrule | Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

## 7. Benennen Sie die Web-API-Anwendung und definieren Sie ihre Ausgabetransformationsregeln mithilfe einer externen Datei.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

### Ablaufzeit des Zugriffstokens aktualisieren

Sie können die Ablaufzeit des Zugriffstokens mit dem PowerShell-Befehl aktualisieren.

### Über diese Aufgabe

- Ein Zugriffstoken kann nur für eine bestimmte Kombination aus Benutzer, Client und Ressource verwendet werden. Zugriffstoken können nicht widerrufen werden und sind bis zu ihrem Ablauf gültig.
- Standardmäßig beträgt die Ablaufzeit eines Zugriffstokens 60 Minuten. Diese minimale Ablaufzeit ist ausreichend und skaliert. Sie müssen einen ausreichenden Wert bereitstellen, um die Ausführung geschäftskritischer Jobs zu vermeiden.

### Schritt

Um die Ablaufzeit des Zugriffstokens für eine Anwendungsgruppen-WebAPI zu aktualisieren, verwenden Sie den folgenden Befehl im AD FS-Server.

```
+
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

### Abrufen des Bearertokens von AD FS

Sie sollten die unten genannten Parameter in einem beliebigen REST-Client (wie Postman) eingeben und werden aufgefordert, die Benutzeranmeldeinformationen einzugeben. Zusätzlich sollten Sie die Zwei-Faktor-Authentifizierung (etwas, das Sie haben und etwas, das Sie sind) eingeben, um das Inhabertoken zu erhalten.



+ Die Gültigkeit des Bearer-Tokens kann vom AD FS-Server pro Anwendung konfiguriert werden und die Standardgültigkeitsdauer beträgt 60 Minuten.

| Feld                     | Wert                                                                                                                                                                         |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zuschussart              | Autorisierungscode                                                                                                                                                           |
| Rückruf-URL              | Geben Sie die Basis-URL Ihrer Anwendung ein, wenn Sie keine Rückruf-URL haben.                                                                                               |
| Authentifizierungs-URL   | [ADFS-Domänenname]/adfs/oauth2/authorize                                                                                                                                     |
| Zugriffstoken-URL        | [ADFS-Domänenname]/adfs/oauth2/token                                                                                                                                         |
| Client-ID                | Geben Sie die AD FS-Client-ID ein                                                                                                                                            |
| Clientgeheimnis          | Geben Sie den geheimen AD FS-Clientschlüssel ein.                                                                                                                            |
| Umfang                   | OpenID                                                                                                                                                                       |
| Client-Authentifizierung | Als Basic AUTH Header senden                                                                                                                                                 |
| Ressource                | Fügen Sie auf der Registerkarte <b>Erweiterte Optionen</b> das Feld „Ressource“ mit demselben Wert wie die Rückruf-URL hinzu, die als „aud“-Wert im JWT-Token enthalten ist. |

### Konfigurieren Sie MFA in SnapCenter Server mit PowerShell, SCCLI und REST-API

Sie können MFA in SnapCenter Server mithilfe von PowerShell, SCCLI und REST API konfigurieren.

#### SnapCenter MFA CLI-Authentifizierung

In PowerShell und SCCLI wird das vorhandene Cmdlet (Open-SmConnection) um ein weiteres Feld namens „AccessToken“ erweitert, um das Bearer-Token zur Authentifizierung des Benutzers zu verwenden.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [ -AccessToken <string>]
```

Nachdem das obige Cmdlet ausgeführt wurde, wird für den jeweiligen Benutzer eine Sitzung erstellt, um weitere SnapCenter -Cmdlets auszuführen.

#### SnapCenter MFA Rest API-Authentifizierung

Verwenden Sie das Bearer-Token im Format *Authorization=Bearer <Zugriffstoken>* im REST-API-Client (wie Postman oder Swagger) und geben Sie den Rollennamen des Benutzers im Header an, um eine erfolgreiche Antwort von SnapCenter zu erhalten.

## MFA Rest API-Workflow

Wenn MFA mit AD FS konfiguriert ist, sollten Sie sich mit einem Zugriffstoken (Bearer-Token) authentifizieren, um über eine beliebige Rest-API auf die SnapCenter -Anwendung zuzugreifen.

### Über diese Aufgabe

- Sie können jeden REST-Client wie Postman, Swagger UI oder FireCamp verwenden.
- Holen Sie sich ein Zugriffstoken und verwenden Sie es zur Authentifizierung nachfolgender Anfragen (SnapCenter Rest API), um beliebige Vorgänge auszuführen.

### Schritte

#### Zur Authentifizierung über AD FS MFA

1. Konfigurieren Sie den REST-Client so, dass er den AD FS-Endpunkt aufruft, um das Zugriffstoken abzurufen.

Wenn Sie auf die Schaltfläche klicken, um ein Zugriffstoken für eine Anwendung zu erhalten, werden Sie zur AD FS-SSO-Seite weitergeleitet, wo Sie Ihre AD-Anmeldeinformationen angeben und sich mit MFA authentifizieren müssen. 1. Geben Sie auf der AD FS-SSO-Seite Ihren Benutzernamen oder Ihre E-Mail-Adresse in das Textfeld „Benutzername“ ein.

+ Benutzernamen müssen als Benutzer@Domäne oder Domäne\Benutzer formatiert sein.

2. Geben Sie im Textfeld „Kennwort“ Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Wählen Sie im Abschnitt **Anmeldeoptionen** eine Authentifizierungsoption aus und authentifizieren Sie sich (je nach Ihrer Konfiguration).
  - Push: Genehmigen Sie die Push-Benachrichtigung, die an Ihr Telefon gesendet wird.
  - QR-Code: Scannen Sie den QR-Code mit der mobilen AUTH Point-App und geben Sie anschließend den in der App angezeigten Bestätigungscode ein.
  - Einmalkennwort: Geben Sie das Einmalkennwort für Ihr Token ein.

5. Nach erfolgreicher Authentifizierung öffnet sich ein Popup, das den Zugriff, die ID und das Aktualisierungstoken enthält.

Kopieren Sie das Zugriffstoken und verwenden Sie es in der SnapCenter Rest API, um den Vorgang auszuführen.

6. In der Rest-API sollten Sie das Zugriffstoken und den Rollennamen im Header-Abschnitt übergeben.
7. SnapCenter validiert dieses Zugriffstoken von AD FS.

Wenn es sich um ein gültiges Token handelt, dekodiert SnapCenter es und erhält den Benutzernamen.

8. Mithilfe des Benutzernamens und des Rollennamens authentifiziert SnapCenter den Benutzer für eine API-Ausführung.

Wenn die Authentifizierung erfolgreich ist, gibt SnapCenter das Ergebnis zurück, andernfalls wird eine Fehlermeldung angezeigt.

## Aktivieren oder deaktivieren Sie die SnapCenter MFA-Funktionalität für Rest API, CLI und GUI

### GUI

#### Schritte

1. Melden Sie sich als SnapCenter -Administrator beim SnapCenter -Server an.
2. Klicken Sie auf **Einstellungen > Globale Einstellungen > MultiFactorAuthentication(MFA)-Einstellungen**
3. Wählen Sie die Schnittstelle (GUI/RST API/CLI) aus, um die MFA-Anmeldung zu aktivieren oder zu deaktivieren.

### PowerShell-Schnittstelle

#### Schritte

1. Führen Sie die PowerShell- oder CLI-Befehle aus, um MFA für GUI, Rest API, PowerShell und SCCLI zu aktivieren.

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

Der Pfadparameter gibt den Speicherort der XML-Datei mit den AD FS MFA-Metadaten an.

Aktiviert MFA für SnapCenter GUI, Rest API, PowerShell und SCCLI, konfiguriert mit dem angegebenen AD FS-Metadatendateipfad.

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe des Get-SmMultiFactorAuthentication Cmdlet.

### SCCLI-Schnittstelle

#### Schritte

1. # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true  
-IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path  
"C:\ADFS\_metadata\abc.xml"
2. # sccli Get-SmMultiFactorAuthentication

### REST-APIs

1. Führen Sie die folgende Post-API aus, um MFA für GUI, Rest-API, PowerShell und SCCLI zu aktivieren.

| Parameter        | Wert                                        |
|------------------|---------------------------------------------|
| Angeforderte URL | /api/4.9/settings/multifactorauthentication |
| HTTP-Methode     | Post                                        |

|                  |                                                                                                                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anforderungstext | { "IsGuiMFAEnabled": false,<br>"IsRestApiMFAEnabled": true, "IsCliMFAEnabled":<br>false, "ADFSConfigFilePath":<br>"C:\\ADFS_metadata\\abc.xml" }                                                                                                        |
| Antworttext      | { "MFAConfiguration": { "IsGuiMFAEnabled": false,<br>"ADFSConfigFilePath":<br>"C:\\ADFS_metadata\\abc.xml",<br>"SCConfigFilePath": null, "IsRestApiMFAEnabled":<br>true, "IsCliMFAEnabled": false, "ADFSHostName":<br>"win-ads-sc49.winscedom2.com" } } |

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe der folgenden API.

| Parameter        | Wert                                                                                                                                                                                                                                                    |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Angeforderte URL | /api/4.9/settings/multifactorauthentication                                                                                                                                                                                                             |
| HTTP-Methode     | Erhalten                                                                                                                                                                                                                                                |
| Antworttext      | { "MFAConfiguration": { "IsGuiMFAEnabled": false,<br>"ADFSConfigFilePath":<br>"C:\\ADFS_metadata\\abc.xml",<br>"SCConfigFilePath": null, "IsRestApiMFAEnabled":<br>true, "IsCliMFAEnabled": false, "ADFSHostName":<br>"win-ads-sc49.winscedom2.com" } } |

## Installieren des SnapCenter -Servers

### Installieren Sie den SnapCenter -Server auf einem Windows-Host

Sie können die ausführbare Datei des SnapCenter Server-Installationsprogramms ausführen, um den SnapCenter Server zu installieren.

Sie können optional mehrere Installations- und Konfigurationsverfahren mithilfe von PowerShell-Cmdlets durchführen. Sie sollten PowerShell 7.4.2 oder höher verwenden.



Die automatische Installation des SnapCenter -Servers über die Befehlszeile wird nicht unterstützt.

#### Bevor Sie beginnen

- Der SnapCenter Server-Host muss über aktuelle Windows-Updates verfügen und darf keine ausstehenden Systemneustarts aufweisen.
- Sie sollten sichergestellt haben, dass MySQL Server nicht auf dem Host installiert ist, auf dem Sie den SnapCenter Server installieren möchten.
- Sie sollten das Debuggen des Windows-Installationsprogramms aktiviert haben.

Informationen zum Aktivieren finden Sie auf der Microsoft-Website "[Protokollierung des Windows-](#)



Sie sollten den SnapCenter -Server nicht auf einem Host installieren, der über Microsoft Exchange Server, Active Directory oder Domain Name Server verfügt.

### Schritte

1. Laden Sie das SnapCenter Server-Installationspaket herunter von "[NetApp Support Site](#)".
2. Starten Sie die Installation des SnapCenter -Servers, indem Sie auf die heruntergeladene EXE-Datei doppelklicken.

Nachdem Sie die Installation gestartet haben, werden alle Vorprüfungen durchgeführt und wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Sie können die Warnmeldungen ignorieren und mit der Installation fortfahren. Fehler sollten jedoch behoben sein.

3. Überprüfen Sie die vorab ausgefüllten Werte, die für die Installation des SnapCenter -Servers erforderlich sind, und ändern Sie sie bei Bedarf.

Sie müssen das Kennwort für die MySQL Server-Repository-Datenbank nicht angeben. Während der Installation des SnapCenter -Servers wird das Kennwort automatisch generiert.



Das Sonderzeichen "%" is not supported in the custom path for the repository database. If you include "%" in the Pfad, die Installation schlägt fehl.

4. Klicken Sie auf **Jetzt installieren**.

Sollten Sie ungültige Werte angegeben haben, werden entsprechende Fehlermeldungen angezeigt. Sie sollten die Werte erneut eingeben und dann die Installation starten.



Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wird der ausgeführte Schritt abgeschlossen und anschließend der Rollback-Vorgang gestartet. Der SnapCenter -Server wird vollständig vom Host entfernt.

Wenn Sie jedoch auf **Abbrechen** klicken, während die Vorgänge „Neustart der SnapCenter Server-Site“ oder „Warten auf den Start des SnapCenter Servers“ ausgeführt werden, wird die Installation fortgesetzt, ohne den Vorgang abzubrechen.

Protokolldateien werden immer (die ältesten zuerst) im Ordner %temp% des Administratorbenutzers aufgelistet. Wenn Sie die Protokollspeicherorte umleiten möchten, starten Sie die Installation des SnapCenter -Servers über die Eingabeaufforderung, indem Sie Folgendes ausführen:  
`C:\installer_location\installer_name.exe /log"C:\\"`

### Während der Installation auf dem Windows-Host aktivierte Funktionen

Das SnapCenter Server-Installationsprogramm aktiviert während der Installation die Windows-Funktionen und -Rollen auf Ihrem Windows-Host. Diese könnten für die Fehlerbehebung und Wartung des Hostsystems von Interesse sein.



| Kategorie | Funktion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Webserver | <ul style="list-style-type: none"> <li>• Internetinformationsdienste</li> <li>• World Wide Web-Dienste</li> <li>• Allgemeine HTTP-Funktionen <ul style="list-style-type: none"> <li>◦ Standarddokument</li> <li>◦ Verzeichnissuche</li> <li>◦ HTTP-Fehler</li> <li>◦ HTTP-Umleitung</li> <li>◦ Statischer Inhalt</li> <li>◦ WebDAV-Veröffentlichung</li> </ul> </li> <li>• Gesundheit und Diagnostik <ul style="list-style-type: none"> <li>◦ Benutzerdefinierte Protokollierung</li> <li>◦ HTTP-Protokollierung</li> <li>◦ Protokollierungstools</li> <li>◦ Anforderungsmonitor</li> <li>◦ Ablaufverfolgung</li> </ul> </li> <li>• Leistungsmerkmale <ul style="list-style-type: none"> <li>◦ Komprimierung statischer Inhalte</li> </ul> </li> <li>• Sicherheit <ul style="list-style-type: none"> <li>◦ IP-Sicherheit</li> <li>◦ Basisauthentifizierung</li> <li>◦ Zentralisierte SSL-Zertifikatunterstützung</li> <li>◦ Client-Zertifikatzuordnungsauthentifizierung</li> <li>◦ Authentifizierung über die IIS-Client-Zertifikatzuordnung</li> <li>◦ IP- und Domänenbeschränkungen</li> <li>◦ Anforderungsfilterung</li> <li>◦ URL-Autorisierung</li> <li>◦ Windows-Authentifizierung</li> </ul> </li> <li>• Funktionen zur Anwendungsentwicklung <ul style="list-style-type: none"> <li>◦ .NET-Erweiterbarkeit 4.5</li> <li>◦ Anwendungsinitialisierung</li> <li>◦ ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>◦ Serverseitige Includes</li> <li>◦ WebSocket-Protokoll</li> </ul> </li> <li>• Verwaltungstools <ul style="list-style-type: none"> <li>◦ IIS-Verwaltungskonsole</li> </ul> </li> </ul> |

| Kategorie                         | Funktion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IIS-Verwaltungsskripts und -Tools | <ul style="list-style-type: none"> <li>• IIS-Verwaltungsdienst</li> <li>• Webverwaltungstools</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                 |
| .NET Framework 8.0.12 Funktionen  | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• Windows Communication Foundation (WCF) HTTP-Aktivierung<sup>45</sup> <ul style="list-style-type: none"> <li>◦ TCP-Aktivierung</li> <li>◦ HTTP-Aktivierung</li> </ul> </li> </ul>                                                                                                                                                                                    |
| Nachrichtenwarteschlange          | <ul style="list-style-type: none"> <li>• Nachrichtenwarteschlangendienste</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>Stellen Sie sicher, dass keine anderen Anwendungen den von SnapCenter erstellten und verwalteten MSMQ-Dienst verwenden.</p> </div> </div> <ul style="list-style-type: none"> <li>• RabbitMQ</li> <li>• Erlang</li> </ul> |
| Windows-Prozessaktivierungsdienst | <ul style="list-style-type: none"> <li>• Prozessmodell</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Konfigurations-APIs               | Alle                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Installieren Sie den SnapCenter -Server auf einem Linux-Host

Sie können die ausführbare Datei des SnapCenter Server-Installationsprogramms ausführen, um den SnapCenter Server zu installieren.

### Bevor Sie beginnen

- Wenn Sie den SnapCenter -Server mit einem Nicht-Root-Benutzer installieren möchten, der nicht über ausreichende Berechtigungen zum Installieren von SnapCenter verfügt, holen Sie sich die Sudoers-Prüfsummendatei von der NetApp Support-Site. Sie sollten basierend auf der Linux-Version eine entsprechende Prüfsummendatei verwenden.
- Wenn das Sudo-Paket in SUSE Linux nicht verfügbar ist, installieren Sie das Sudo-Paket, um Authentifizierungsfehler zu vermeiden.
- Konfigurieren Sie für SUSE Linux den Hostnamen, um Installationsfehler zu vermeiden.
- Überprüfen Sie den sicheren Linux-Status, indem Sie den Befehl ausführen `sestatus`. Wenn der *SELinux-Status* „aktiviert“ und der *aktuelle Modus* „erzwingen“ ist, führen Sie Folgendes aus:
  - Führen Sie den folgenden Befehl aus: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

Der Standardwert von *WEBAPP\_EXTERNAL\_PORT* ist 8146



- Wenn die Firewall den Port blockiert, führen Sie `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT>/tcp`

Der Standardwert von `WEBAPP_EXTERNAL_PORT` ist 8146

- Führen Sie die folgenden Befehle aus dem Verzeichnis aus, für das Sie Lese- und Schreibberechtigung haben:
  - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

Wenn der Befehl „keine Aktion“ zurückgibt, führen Sie den Befehl nach der Installation von SnapCenter Server erneut aus.

  - Wenn der Befehl `my-nginx.pp` erstellt, führen Sie den Befehl aus, um das Richtlinienpaket zu aktivieren: `sudo semodule -i my-nginx.pp`
- Der für das MySQL-PID-Verzeichnis verwendete Pfad ist `/var/opt/mysqld`. Führen Sie die folgenden Befehle aus, um die Berechtigungen für die MySQL-Installation festzulegen.
  - `mkdir /var/opt/mysqld`
  - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
  - `sudo restorecon -Rv /var/opt/mysqld`
- Der für das MySQL-Datenverzeichnis verwendete Pfad lautet `/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/`. Führen Sie die folgenden Befehle aus, um die Berechtigungen für das MySQL-Datenverzeichnis festzulegen.
  - `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
  - `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
  - `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

### Informationen zu diesem Vorgang

- Wenn SnapCenter Server auf dem Linux-Host installiert wird, werden Dienste von Drittanbietern wie MySQL, RabbitMq und Erlang installiert. Sie sollten sie nicht deinstallieren.
- Der auf dem Linux-Host installierte SnapCenter -Server unterstützt Folgendes nicht:
  - Hochverfügbarkeit
  - Windows-Plug-Ins
  - Active Directory (Unterstützt nur lokale Benutzer, sowohl Root- als auch Nicht-Root-Benutzer mit Anmeldeinformationen)
  - Schlüsselbasierte Authentifizierung zur Anmeldung bei SnapCenter
- Wenn während der Installation der .NET-Laufzeit die Abhängigkeiten der Bibliothek *libicu* nicht aufgelöst werden können, installieren Sie *libicu*, indem Sie den folgenden Befehl ausführen: `yum install -y libicu`
- Wenn die Installation von SnapCenter Server aufgrund der Nichtverfügbarkeit von *Perl* fehlschlägt, installieren Sie *Perl*, indem Sie den folgenden Befehl ausführen: `yum install -y perl`

### Schritte

1. Laden Sie Folgendes herunter von ["NetApp Support Site"](#) in das `/Home-Verzeichnis`.

- SnapCenter Server-Installationspaket – **snapcenter-linux-server-(el8/el9/sles15).bin**
- Öffentliche Schlüsseldatei – **snapcenter\_public\_key.pub**
- Entsprechende Signaturdatei – **snapcenter-linux-server-(el8/el9/sles15).bin.sig**

2. Validieren Sie die Signaturdatei.

```
$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>
```

3. Fügen Sie für die Installation durch einen Nicht-Root-Benutzer den in **snapcenter\_server\_checksum\_(el8/el9/sles15).txt** angegebenen Visudo-Inhalt hinzu, der zusammen mit dem .bin-Installationsprogramm verfügbar ist.

4. Weisen Sie die Ausführungsberechtigung für das .bin-Installationsprogramm zu.

```
chmod +x snapcenter-linux-server-(el8/el9/sles15).bin
```

5. Führen Sie eine der Aktionen aus, um SnapCenter Server zu installieren.

| Wenn Sie auftreten möchten ... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interaktive Installation       | <pre>./snapcenter-linux-server-(el8/el9/sles15).bin</pre> <p>Sie werden aufgefordert, die folgenden Angaben einzugeben:</p> <ul style="list-style-type: none"> <li>• Der externe Port der Webanwendung, der für den Zugriff auf den SnapCenter -Server außerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8146.</li> <li>• Der SnapCenter Server-Benutzer, der SnapCenter Server installieren wird.</li> <li>• Das Installationsverzeichnis, in dem Pakete installiert werden.</li> </ul> |

| Wenn Sie auftreten möchten ... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nicht interaktive Installation | <pre data-bbox="842 163 1364 478">sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=&lt;port&gt; -DWEBAPP_INTERNAL_PORT=&lt;port&gt; -DSMCORE_PORT=&lt;port&gt; -DSCHEDULER_PORT=&lt;port&gt; -DSNAPCENTER_SERVER_USER=&lt;user&gt; -DUSER_INSTALL_DIR=&lt;dir&gt; -DINSTALL_LOG_NAME=&lt;filename&gt;</pre> <p data-bbox="842 514 1479 682">Beispiel: <code>sudo ./snapcenter_linux_server.bin -i silent</code><br/> <code>-DWEBAPP_EXTERNAL_PORT=8146</code><br/> <code>-DSNAPCENTER_SERVER_USER=root</code><br/> <code>-DUSER_INSTALL_DIR=/opt</code><br/> <code>-DINSTALL_LOG_NAME=InstallerLog.log</code></p> <p data-bbox="842 718 1443 783">Protokolle werden unter <code>/var/opt/snapcenter/logs</code> gespeichert.</p> <p data-bbox="842 819 1406 884">Für die Installation von SnapCenter Server zu übergebende Parameter:</p> <ul data-bbox="867 919 1479 2068" style="list-style-type: none"> <li>• <code>DWEBAPP_EXTERNAL_PORT</code>: Externer Webapp-Port, der für den Zugriff auf den SnapCenter -Server außerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8146.</li> <li>• <code>DWEBAPP_INTERNAL_PORT</code>: Interner Webapp-Port, der für den Zugriff auf den SnapCenter -Server innerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8147.</li> <li>• <code>DSMCORE_PORT</code>: SMCore-Port, auf dem die SMCore-Dienste ausgeführt werden. Der Standardwert ist 8145.</li> <li>• <code>DSCHEDULER_PORT</code>: Scheduler-Port, auf dem die Scheduler-Dienste ausgeführt werden. Der Standardwert ist 8154.</li> <li>• <code>DSNAPCENTER_SERVER_USER</code>: SnapCenter Server-Benutzer, der SnapCenter Server installieren wird. Für <code>DSNAPCENTER_SERVER_USER</code> ist der Standard der Benutzer, der das Installationsprogramm ausführt.</li> <li>• <code>DUSER_INSTALL_DIR</code>: Installationsverzeichnis, in dem Pakete installiert werden. Für <code>DUSER_INSTALL_DIR</code> ist das Standardinstallationsverzeichnis <code>/opt</code>.</li> <li>• <code>DINSTALL_LOG_NAME</code>: Name der Protokolldatei, in der die Installationsprotokolle gespeichert werden. Dies ist ein optionaler Parameter. Wenn dieser Parameter angegeben wird, werden keine Protokolle auf der Konsole angezeigt. Wenn Sie diesen Parameter nicht angeben, werden Protokolle auf der Konsole</li> </ul> |

## Wie geht es weiter?

- Wenn der *SELinux-Status* „aktiviert“ und der *aktuelle Modus* „erzwingen“ ist, kann der **nginx**-Dienst nicht gestartet werden. Sie sollten die folgenden Befehle ausführen:
  - a. Gehen Sie zum Home-Verzeichnis.
  - b. Führen Sie den folgenden Befehl aus: `journalctl -r -u nginx`
  - c. Wenn der interne Port der Webanwendung (8147) nicht lauschen darf, führen Sie die folgenden Befehle aus:
    - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
    - `semodule -i my-nginx.pp`
  - d. Laufen `setsebool -P httpd_can_network_connect`
- DSELINUX: Wenn der *SELinux-Status* „aktiviert“ ist, der *aktuelle Modus* „erzwingen“ ist und Sie die im Abschnitt „Bevor Sie beginnen“ genannten Befehle ausgeführt haben, sollten Sie diesen Parameter angeben und den Wert 1 zuweisen. Der Standardwert ist 0.
- DUPGRADE: Der Standardwert ist 0. Geben Sie diesen Parameter und seinen Wert als eine beliebige Ganzzahl ungleich 0 an, um den SnapCenter -Server zu aktualisieren.

## Während der Installation auf dem Linux-Host aktivierte Funktionen

Der SnapCenter -Server installiert die folgenden Softwarepakete, die bei der Fehlerbehebung und Wartung des Hostsystems helfen können.

- Rabbitmq
- Erlang

## SnapCenter registrieren

Wenn Sie mit NetApp -Produkten noch nicht vertraut sind und noch kein NetApp -Konto besitzen, sollten Sie SnapCenter registrieren, um Support zu erhalten.

### Schritte

1. Navigieren Sie nach der Installation von SnapCenter zu **Hilfe > Info**.
2. Notieren Sie sich im Dialogfeld „Über SnapCenter“ die SnapCenter Instanz, eine 20-stellige Nummer, die mit 971 beginnt.
3. Klicken <https://register.netapp.com>.
4. Klicken Sie auf **Ich bin kein registrierter NetApp -Kunde**.
5. Geben Sie Ihre Daten ein, um sich zu registrieren.
6. Lassen Sie das Feld „NetApp -Referenz-SN“ leer.
7. Wählen Sie \* SnapCenter\* aus der Dropdown-Liste „Produktlinie“ aus.
8. Wählen Sie den Abrechnungsanbieter aus.
9. Geben Sie die 20-stellige SnapCenter Instanz-ID ein.
10. Klicken Sie auf **Senden**.

## Melden Sie sich mit der RBAC-Autorisierung bei SnapCenter an

SnapCenter unterstützt die rollenbasierte Zugriffskontrolle (RBAC). Der SnapCenter Administrator weist Rollen und Ressourcen über SnapCenter RBAC entweder einem Benutzer in der Arbeitsgruppe oder im Active Directory oder Gruppen im Active Directory zu. Der RBAC-Benutzer kann sich jetzt mit den zugewiesenen Rollen bei SnapCenter anmelden.

## Bevor Sie beginnen

- Sie sollten den Windows Process Activation Service (WAS) im Windows Server Manager aktivieren.
- Wenn Sie Internet Explorer als Browser zum Anmelden beim SnapCenter -Server verwenden möchten, sollten Sie sicherstellen, dass der geschützte Modus im Internet Explorer deaktiviert ist.
- Wenn SnapCenter Server auf einem Linux-Host installiert ist, sollten Sie sich mit dem Benutzerkonto anmelden, das für die Installation von SnapCenter Server verwendet wurde.

## Über diese Aufgabe

Während der Installation erstellt der SnapCenter Server-Installationsassistent eine Verknüpfung und platziert sie auf dem Desktop und im Startmenü des Hosts, auf dem SnapCenter installiert ist. Darüber hinaus zeigt der Installationsassistent am Ende der Installation die SnapCenter -URL basierend auf den Informationen an, die Sie während der Installation angegeben haben. Diese können Sie kopieren, wenn Sie sich von einem Remote-System aus anmelden möchten.



Wenn in Ihrem Webbrowser mehrere Registerkarten geöffnet sind, werden Sie durch das Schließen der SnapCenter -Browserregisterkarte nicht von SnapCenter abgemeldet. Um Ihre Verbindung mit SnapCenter zu beenden, müssen Sie sich von SnapCenter abmelden, indem Sie entweder auf die Schaltfläche **Abmelden** klicken oder den gesamten Webbrowser schließen.

**Best Practice:** Aus Sicherheitsgründen wird empfohlen, dass Sie in Ihrem Browser nicht die Möglichkeit aktivieren, Ihr SnapCenter -Passwort zu speichern.

Die Standard-GUI-URL ist eine sichere Verbindung zum Standardport 8146 auf dem Server, auf dem der SnapCenter -Server installiert ist (<https://server:8146>). Wenn Sie während der SnapCenter -Installation einen anderen Serverport angegeben haben, wird stattdessen dieser Port verwendet.

Für die Bereitstellung mit hoher Verfügbarkeit (HA) müssen Sie über die IP des virtuellen Clusters [https://Virtual\\_Cluster\\_IP\\_or\\_FQDN:8146](https://Virtual_Cluster_IP_or_FQDN:8146) auf SnapCenter zugreifen. Wenn die SnapCenter -Benutzeroberfläche nicht angezeigt wird, wenn Sie im Internet Explorer (IE) zu [https://Virtual\\_Cluster\\_IP\\_or\\_FQDN:8146](https://Virtual_Cluster_IP_or_FQDN:8146) navigieren, müssen Sie die IP-Adresse oder den FQDN des virtuellen Clusters als vertrauenswürdige Site im IE auf jedem Plug-In-Host hinzufügen oder die erweiterte Sicherheit des IE auf jedem Plug-In-Host deaktivieren. Weitere Informationen finden Sie unter ["Von außerhalb des Netzwerks kann nicht auf die Cluster-IP-Adresse zugegriffen werden"](#).

Zusätzlich zur Verwendung der SnapCenter -GUI können Sie PowerShell-Cmdlets verwenden, um Skripts zum Durchführen von Konfigurations-, Sicherungs- und Wiederherstellungsvorgängen zu erstellen. Einige Cmdlets haben sich möglicherweise mit jeder SnapCenter Version geändert. Der ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) hat die Details.



Wenn Sie sich zum ersten Mal bei SnapCenter anmelden, müssen Sie sich mit den Anmeldeinformationen anmelden, die Sie während des Installationsvorgangs angegeben haben.

## Schritte

1. Starten Sie SnapCenter über die Verknüpfung auf Ihrem lokalen Host-Desktop, über die URL, die am Ende der Installation bereitgestellt wird, oder über die URL, die Sie von Ihrem SnapCenter Administrator erhalten haben.
2. Geben Sie die Benutzeranmeldeinformationen ein.

| Um Folgendes anzugeben ... | Verwenden Sie eines dieser Formate ...                                                                                                                                                                                             |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domänenadministrator       | <ul style="list-style-type: none"> <li>• NetBIOS\Benutzername</li> <li>• Benutzername@UPN-Suffix</li> </ul> <p>Beispiel: Benutzername@netapp.com</p> <ul style="list-style-type: none"> <li>• Domänen-FQDN\Benutzername</li> </ul> |
| Lokaler Administrator      | Benutzername                                                                                                                                                                                                                       |

3. Wenn Ihnen mehr als eine Rolle zugewiesen ist, wählen Sie im Feld „Rolle“ die Rolle aus, die Sie für diese Anmeldesitzung verwenden möchten.

Ihr aktueller Benutzer und die zugehörige Rolle werden nach der Anmeldung oben rechts im SnapCenter angezeigt.

## Ergebnis

Die Dashboard-Seite wird angezeigt.

Wenn die Protokollierung mit der Fehlermeldung fehlschlägt, dass die Site nicht erreicht werden kann, sollten Sie das SSL-Zertifikat SnapCenter zuordnen. ["Mehr erfahren"](#)

## Nachdem Sie fertig sind

Aktualisieren Sie die Ressourcenliste, nachdem Sie sich zum ersten Mal als RBAC-Benutzer beim SnapCenter -Server angemeldet haben.

Wenn Sie nicht vertrauenswürdige Active Directory-Domänen haben, die von SnapCenter unterstützt werden sollen, müssen Sie diese Domänen bei SnapCenter registrieren, bevor Sie die Rollen für die Benutzer in nicht vertrauenswürdigen Domänen konfigurieren. ["Mehr erfahren"](#) .

Wenn Sie den Plug-in-Host in SnapCenter hinzufügen möchten, das auf einem Linux-Host ausgeführt wird, sollten Sie die Prüfsummendatei vom Speicherort abrufen: */opt/NetApp/snapcenter/SnapManagerWeb/Repository*.

Ab Version 6.0 wird auf dem Desktop eine Verknüpfung für SnapCenter PowerShell erstellt. Sie können über die Verknüpfung direkt auf die SnapCenter PowerShell-Cmdlets zugreifen.

## Melden Sie sich mit der Multi-Faktor-Authentifizierung (MFA) bei SnapCenter an.

SnapCenter Server unterstützt MFA für Domänenkonten, die Teil des Active Directory sind.

## Bevor Sie beginnen

Sie sollten MFA aktiviert haben. Informationen zum Aktivieren von MFA finden Sie unter ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#)

## Über diese Aufgabe

- Nur FQDN wird unterstützt
- Arbeitsgruppen- und domänenübergreifende Benutzer können sich nicht mit MFA anmelden

## Schritte

1. Starten Sie SnapCenter über die Verknüpfung auf Ihrem lokalen Host-Desktop, über die URL, die am Ende der Installation bereitgestellt wird, oder über die URL, die Sie von Ihrem SnapCenter Administrator erhalten haben.
2. Geben Sie auf der AD FS-Anmeldeseite Benutzernamen und Kennwort ein.

Wenn auf der AD FS-Seite die Fehlermeldung „Benutzername oder Kennwort ungültig“ angezeigt wird, sollten Sie Folgendes überprüfen:

- Ob der Benutzername oder das Passwort gültig ist

Das Benutzerkonto sollte im Active Directory (AD) vorhanden sein

- Ob Sie die in AD festgelegte maximal zulässige Anzahl von Versuchen überschritten haben
- Ob AD und AD FS aktiv sind

## Ändern Sie das SnapCenter -Standard-GUI-Sitzungstimeout

Sie können die Zeitüberschreitungsdauer der SnapCenter -GUI-Sitzung ändern, um sie kürzer oder länger als die Standardzeitüberschreitungsdauer von 20 Minuten zu machen.

Als Sicherheitsfunktion warnt SnapCenter Sie nach einer Standardzeit von 15 Minuten Inaktivität, dass Sie in 5 Minuten von der GUI-Sitzung abgemeldet werden. Standardmäßig meldet SnapCenter Sie nach 20 Minuten Inaktivität von der GUI-Sitzung ab und Sie müssen sich erneut anmelden.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen > Globale Einstellungen**.
2. Klicken Sie auf der Seite „Globale Einstellungen“ auf **Konfigurationseinstellungen**.
3. Geben Sie im Feld „Sitzungstimeout“ das neue Sitzungstimeout in Minuten ein und klicken Sie dann auf **Speichern**.

## Sichern Sie den SnapCenter -Webserver, indem Sie SSL 3.0 deaktivieren

Aus Sicherheitsgründen sollten Sie das Secure Socket Layer (SSL) 3.0-Protokoll in Microsoft IIS deaktivieren, wenn es auf Ihrem SnapCenter -Webserver aktiviert ist.

Das SSL 3.0-Protokoll weist Fehler auf, die ein Angreifer ausnutzen kann, um Verbindungsfehler zu verursachen oder Man-in-the-Middle-Angriffe durchzuführen und den verschlüsselten Datenverkehr zwischen Ihrer Website und ihren Besuchern zu beobachten.

## Schritte

1. Um den Registrierungseditor auf dem SnapCenter -Webserver-Host zu starten, klicken Sie auf **Start > Ausführen** und geben Sie dann regedit ein.
2. Navigieren Sie im Registrierungs-Editor zu  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\
  - Wenn der Serverschlüssel bereits vorhanden ist:
    - i. Wählen Sie das aktivierte DWORD aus und klicken Sie dann auf **Bearbeiten > Ändern**.

- ii. Ändern Sie den Wert auf 0 und klicken Sie dann auf **OK**.
- Wenn der Serverschlüssel nicht vorhanden ist:
  - i. Klicken Sie auf **Bearbeiten > Neu > Schlüssel** und benennen Sie den Schlüssel dann „Server“.
  - ii. Klicken Sie bei ausgewähltem neuen Serverschlüssel auf **Bearbeiten > Neu > DWORD**.
  - iii. Benennen Sie das neue DWORD „Enabled“ und geben Sie dann 0 als Wert ein.

3. Schließen Sie den Registrierungseditor.

## Konfigurieren des SnapCenter -Servers

### Hinzufügen und Bereitstellen des Speichersystems

#### Speichersysteme hinzufügen

Sie sollten das Speichersystem einrichten, das SnapCenter Zugriff auf ONTAP -Speicher, ASA r2-Systeme oder Amazon FSx for NetApp ONTAP gewährt, um Datenschutz- und Bereitstellungsvorgänge durchzuführen.

Sie können entweder eine eigenständige SVM oder einen Cluster aus mehreren SVMs hinzufügen. Wenn Sie Amazon FSx for NetApp ONTAP verwenden, können Sie entweder FSx-Admin-LIF hinzufügen, das aus mehreren SVMs besteht, indem Sie das fsxadmin-Konto verwenden, oder FSx-SVM in SnapCenter hinzufügen.

#### Bevor Sie beginnen

- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

#### Über diese Aufgabe

- Wenn Sie Speichersysteme konfigurieren, können Sie auch die Funktionen Event Management System (EMS) und AutoSupport aktivieren. Das AutoSupport Tool sammelt Daten zum Zustand Ihres Systems und sendet die Daten automatisch an den technischen Support von NetApp , damit dieser Fehler an Ihrem System beheben kann.

Wenn Sie diese Funktionen aktivieren, sendet SnapCenter AutoSupport Informationen an das Speichersystem und EMS-Nachrichten an das Syslog des Speichersystems, wenn eine Ressource geschützt ist, ein Wiederherstellungs- oder Klonvorgang erfolgreich abgeschlossen wird oder ein Vorgang fehlschlägt.



- Wenn Sie Snapshots auf ein SnapMirror oder SnapVault -Ziel replizieren möchten, müssen Sie Speichersystemverbindungen für die Ziel-SVM oder den Ziel-Cluster sowie die Quell-SVM oder den Quell-Cluster einrichten.



Wenn Sie das Kennwort des Speichersystems ändern, können geplante Jobs, On-Demand-Sicherungs- und Wiederherstellungsvorgänge fehlschlagen. Nachdem Sie das Kennwort des Speichersystems geändert haben, können Sie das Kennwort aktualisieren, indem Sie auf der Registerkarte „Speicher“ auf „Ändern“ klicken.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Klicken Sie auf der Seite „Speichersysteme“ auf **Neu**.
3. Geben Sie auf der Seite „Speichersystem hinzufügen“ die folgenden Informationen ein:

| Für dieses Feld...    | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Speichersystem        | <p data-bbox="842 159 1435 226">Geben Sie den Namen oder die IP-Adresse des Speichersystems ein.</p> <div data-bbox="873 415 927 468">  </div> <p data-bbox="989 275 1443 611">Speichersystemnamen dürfen (ohne Domännennamen) höchstens 15 Zeichen lang sein und müssen auflösbar sein. Um Speichersystemverbindungen mit Namen zu erstellen, die mehr als 15 Zeichen haben, können Sie das Cmdlet Add-SmStorageConnectionPowerShell verwenden.</p> <div data-bbox="873 741 927 793">  </div> <p data-bbox="989 667 1422 867">Für Speichersysteme mit MetroCluster -Konfiguration (MCC) wird empfohlen, sowohl lokale als auch Peer-Cluster für unterbrechungsfreie Vorgänge zu registrieren.</p> <p data-bbox="842 915 1484 1045">SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss einen eindeutigen Namen haben.</p> <div data-bbox="873 1150 927 1203">  </div> <p data-bbox="989 1094 1435 1255">Nachdem Sie die Speicherverbindung zu SnapCenter hinzugefügt haben, sollten Sie die SVM oder den Cluster nicht mit ONTAP umbenennen.</p> <div data-bbox="873 1360 927 1413">  </div> <p data-bbox="989 1318 1446 1451">Wenn SVM mit einem Kurznamen oder FQDN hinzugefügt wird, muss es sowohl vom SnapCenter als auch vom Plug-In-Host auflösbar sein.</p> |
| Benutzername/Passwort | <p data-bbox="842 1514 1463 1644">Geben Sie die Anmeldeinformationen des Speicherbenutzers ein, der über die erforderlichen Berechtigungen für den Zugriff auf das Speichersystem verfügt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Für dieses Feld...                                           | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Event Management System (EMS) und AutoSupport -Einstellungen | <p>Wenn Sie EMS-Nachrichten an das Syslog des Speichersystems senden möchten oder wenn Sie möchten, dass AutoSupport Nachrichten zum angewendeten Schutz, zu abgeschlossenen Wiederherstellungsvorgängen oder zu fehlgeschlagenen Vorgängen an das Speichersystem gesendet werden, aktivieren Sie das entsprechende Kontrollkästchen.</p> <p>Wenn Sie das Kontrollkästchen * AutoSupport -Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden* aktivieren, wird auch das Kontrollkästchen * SnapCenter -Server -Ereignisse in Syslog protokollieren* aktiviert, da EMS-Messaging erforderlich ist, um AutoSupport Benachrichtigungen zu aktivieren.</p> |

4. Klicken Sie auf **Weitere Optionen**, wenn Sie die der Plattform, dem Protokoll, dem Port und dem Timeout zugewiesenen Standardwerte ändern möchten.

a. Wählen Sie unter „Plattform“ eine der Optionen aus der Dropdownliste aus.

Wenn es sich bei der SVM um das sekundäre Speichersystem in einer Sicherheitsbeziehung handelt, aktivieren Sie das Kontrollkästchen **Sekundär**. Wenn die Option **Sekundär** ausgewählt ist, führt SnapCenter nicht sofort eine Lizenzprüfung durch.

Wenn Sie SVM in SnapCenter hinzugefügt haben, muss der Benutzer den Plattfortmtpy manuell aus der Dropdown-Liste auswählen.

a. Wählen Sie unter „Protokoll“ das Protokoll aus, das während der SVM- oder Cluster-Einrichtung konfiguriert wurde, normalerweise HTTPS.

b. Geben Sie den Port ein, den das Speichersystem akzeptiert.

Normalerweise funktioniert der Standardport 443.

c. Geben Sie die Zeit in Sekunden ein, die vergehen soll, bevor Kommunikationsversuche abgebrochen werden.

Der Standardwert beträgt 60 Sekunden.

d. Wenn die SVM über mehrere Verwaltungsschnittstellen verfügt, aktivieren Sie das Kontrollkästchen **Bevorzugte IP** und geben Sie dann die bevorzugte IP-Adresse für SVM-Verbindungen ein.

e. Klicken Sie auf **Speichern**.

5. Klicken Sie auf **Senden**.

## Ergebnis

Führen Sie auf der Seite „Speichersysteme“ im Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

- Wählen Sie \* ONTAP SVMs\*, wenn Sie alle hinzugefügten SVMs anzeigen möchten.

Wenn Sie FSx SVMs hinzugefügt haben, werden die FSx SVMs hier aufgelistet.

- Wählen Sie \* ONTAP -Cluster\* aus, wenn Sie alle hinzugefügten Cluster anzeigen möchten.

Wenn Sie FSx-Cluster mit fsxadmin hinzugefügt haben, werden die FSx-Cluster hier aufgelistet.

Wenn Sie auf den Clusternamen klicken, werden alle SVMs, die Teil des Clusters sind, im Abschnitt „Storage Virtual Machines“ angezeigt.

Wenn dem ONTAP Cluster mithilfe der ONTAP GUI ein neues SVM hinzugefügt wird, klicken Sie auf **Neu erkennen**, um das neu hinzugefügte SVM anzuzeigen.

## Nachdem Sie fertig sind

Ein Clusteradministrator muss AutoSupport auf jedem Speichersystemknoten aktivieren, um E-Mail-Benachrichtigungen von allen Speichersystemen zu senden, auf die SnapCenter Zugriff hat, indem er den folgenden Befehl von der Befehlszeile des Speichersystems aus ausführt:

```
autosupport trigger modify -node nodename -autosupport-message client.app.info  
-to enable -noteto enable
```



Der Administrator der Storage Virtual Machine (SVM) hat keinen Zugriff auf AutoSupport.

## Speicherverbindungen und Anmeldeinformationen

Bevor Sie Datenschutzvorgänge durchführen, sollten Sie die Speicherverbindungen einrichten und die Anmeldeinformationen hinzufügen, die der SnapCenter Server und die SnapCenter Plug-Ins verwenden werden.

### Speicherverbindungen

Die Speicherverbindungen ermöglichen dem SnapCenter Server und den SnapCenter -Plug-Ins den Zugriff auf den ONTAP -Speicher. Zum Einrichten dieser Verbindungen gehört auch die Konfiguration der Funktionen von AutoSupport und Event Management System (EMS).

### Anmeldeinformationen

- Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe

Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:

- *NetBIOS\Benutzername*
- *Domänen-FQDN\Benutzername*
- *Benutzername@upn*

- Lokaler Administrator (nur für Arbeitsgruppen)

Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist.

Das gültige Format für das Feld „Benutzername“ ist: *Benutzername*

- Anmeldeinformationen für einzelne Ressourcengruppen

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

## Bereitstellen von Speicher auf Windows-Hosts

### Erstellen und Verwalten von igroups

Sie erstellen Initiatorgruppen (igroups), um anzugeben, welche Hosts auf eine bestimmte LUN im Speichersystem zugreifen können. Sie können SnapCenter verwenden, um eine igroup auf einem Windows-Host zu erstellen, umzubenennen, zu ändern oder zu löschen.

### Erstellen einer igroup

Sie können SnapCenter verwenden, um eine igroup auf einem Windows-Host zu erstellen. Die igroup ist im Assistenten „Datenträger erstellen“ oder „Datenträger verbinden“ verfügbar, wenn Sie die igroup einer LUN zuordnen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Igroup**.
3. Klicken Sie auf der Seite „Initiatorgruppen“ auf **Neu**.
4. Definieren Sie im Dialogfeld „Igroup erstellen“ die Igroup:

| In diesem Bereich... | Machen Sie Folgendes...                                                  |
|----------------------|--------------------------------------------------------------------------|
| Speichersystem       | Wählen Sie die SVM für die LUN aus, die Sie der igroup zuordnen möchten. |
| Gastgeber            | Wählen Sie den Host aus, auf dem Sie die igroup erstellen möchten.       |
| Igroup-Name          | Geben Sie den Namen der Igroup ein.                                      |
| Initiatoren          | Wählen Sie den Initiator aus.                                            |
| Typ                  | Wählen Sie den Initiatortyp: iSCSI, FCP oder gemischt (FCP und iSCSI).   |

5. Wenn Sie mit Ihren Eingaben zufrieden sind, klicken Sie auf **OK**.

SnapCenter erstellt die igroup auf dem Speichersystem.

## Umbenennen einer igroup

Sie können SnapCenter verwenden, um eine vorhandene igroup umzubenennen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Igroup**.
3. Klicken Sie auf der Seite „Initiatorgruppen“ in das Feld **Storage Virtual Machine**, um eine Liste der verfügbaren SVMs anzuzeigen, und wählen Sie dann die SVM für die Igroup aus, die Sie umbenennen möchten.
4. Wählen Sie in der Liste der igroups für die SVM die igroup aus, die Sie umbenennen möchten, und klicken Sie auf **Umbenennen**.
5. Geben Sie im Dialogfeld „igroup umbenennen“ den neuen Namen für die igroup ein und klicken Sie auf **Umbenennen**.

## Ändern einer igroup

Sie können SnapCenter verwenden, um einer vorhandenen Igroup Igroup-Initiatoren hinzuzufügen. Beim Erstellen einer igroup können Sie nur einen Host hinzufügen. Wenn Sie eine Igroup für einen Cluster erstellen möchten, können Sie die Igroup ändern, um dieser Igroup weitere Knoten hinzuzufügen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Igroup**.
3. Klicken Sie auf der Seite „Initiatorgruppen“ in das Feld **Storage Virtual Machine**, um eine Dropdown-Liste der verfügbaren SVMs anzuzeigen, und wählen Sie dann die SVM für die Igroup aus, die Sie ändern möchten.
4. Wählen Sie in der Liste der igroups eine igroup aus und klicken Sie auf **Initiator zu igroup hinzufügen**.
5. Wählen Sie einen Host aus.
6. Wählen Sie die Initiatoren aus und klicken Sie auf **OK**.

## Löschen einer igroup

Sie können SnapCenter verwenden, um eine Igroup zu löschen, wenn Sie sie nicht mehr benötigen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Igroup**.
3. Klicken Sie auf der Seite „Initiatorgruppen“ in das Feld **Storage Virtual Machine**, um eine Dropdown-Liste der verfügbaren SVMs anzuzeigen, und wählen Sie dann die SVM für die Igroup aus, die Sie löschen möchten.
4. Wählen Sie in der Liste der igroups für die SVM die igroup aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
5. Klicken Sie im Dialogfeld „igroup löschen“ auf **OK**.

SnapCenter löscht die igroup.

Der Windows-Host sieht LUNs auf Ihrem Speichersystem als virtuelle Datenträger. Sie können SnapCenter verwenden, um eine FC- oder iSCSI-verbundene LUN zu erstellen und zu konfigurieren.

- SnapCenter unterstützt nur Basisdatenträger. Die dynamischen Datenträger werden nicht unterstützt.
- Für GPT ist nur eine Datenpartition und für MBR eine primäre Partition zulässig, die über ein mit NTFS oder CSVFS formatiertes Volume und einen Mount-Pfad verfügt.
- Unterstützte Partitionsstile: GPT, MBR; in einer VMware UEFI VM werden nur iSCSI-Festplatten unterstützt



SnapCenter unterstützt das Umbenennen einer Festplatte nicht. Wenn eine von SnapCenter verwaltete Festplatte umbenannt wird, sind SnapCenter -Vorgänge nicht erfolgreich.

### Anzeigen der Festplatten auf einem Host

Sie können die Festplatten auf jedem Windows-Host anzeigen, den Sie mit SnapCenter verwalten.

#### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

Die Datenträger werden aufgelistet.

### Anzeigen von Clusterdatenträgern

Sie können Cluster-Datenträger auf dem Cluster anzeigen, den Sie mit SnapCenter verwalten. Die gruppierten Datenträger werden nur angezeigt, wenn Sie den Cluster aus der Dropdown-Liste „Hosts“ auswählen.

#### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Cluster aus der Dropdown-Liste **Host** aus.

Die Datenträger werden aufgelistet.

### Richten Sie eine iSCSI-Sitzung ein

Wenn Sie iSCSI zum Herstellen einer Verbindung mit einer LUN verwenden, müssen Sie vor dem Erstellen der LUN eine iSCSI-Sitzung einrichten, um die Kommunikation zu ermöglichen.

#### Bevor Sie beginnen

- Sie müssen den Speichersystemknoten als iSCSI-Ziel definiert haben.
- Sie müssen den iSCSI-Dienst auf dem Speichersystem gestartet haben. ["Mehr erfahren"](#)

### Über diese Aufgabe

Sie können eine iSCSI-Sitzung nur zwischen denselben IP-Versionen herstellen, entweder von IPv6 zu IPv6 oder von IPv4 zu IPv4.

Sie können eine Link-Local-IPv6-Adresse für die iSCSI-Sitzungsverwaltung und für die Kommunikation zwischen einem Host und einem Ziel nur verwenden, wenn sich beide im selben Subnetz befinden.

Wenn Sie den Namen eines iSCSI-Initiators ändern, wirkt sich dies auf den Zugriff auf iSCSI-Ziele aus. Nach der Namensänderung müssen Sie möglicherweise die vom Initiator aufgerufenen Ziele neu konfigurieren, damit sie den neuen Namen erkennen können. Sie müssen sicherstellen, dass der Host neu gestartet wird, nachdem Sie den Namen eines iSCSI-Initiators geändert haben.

Wenn Ihr Host über mehr als eine iSCSI-Schnittstelle verfügt, können Sie, nachdem Sie eine iSCSI-Sitzung zu SnapCenter mithilfe einer IP-Adresse auf der ersten Schnittstelle hergestellt haben, keine iSCSI-Sitzung von einer anderen Schnittstelle mit einer anderen IP-Adresse herstellen.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **iSCSI-Sitzung**.
3. Wählen Sie aus der Dropdown-Liste **Storage Virtual Machine** die Storage Virtual Machine (SVM) für das iSCSI-Ziel aus.
4. Wählen Sie aus der Dropdown-Liste **Host** den Host für die Sitzung aus.
5. Klicken Sie auf **Sitzung herstellen**.

Der Assistent zum Einrichten einer Sitzung wird angezeigt.

6. Identifizieren Sie im Assistenten „Sitzung einrichten“ das Ziel:

| In diesem Bereich...         | Eingeben...                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Zielknotenname               | Der Knotenname des iSCSI-Ziels<br><br>Wenn ein Zielknotenname vorhanden ist, wird der Name im schreibgeschützten Format angezeigt. |
| Zielportaladresse            | Die IP-Adresse des Zielnetzwerkportals                                                                                             |
| Zielportal-Port              | Der TCP-Port des Zielnetzwerkportals                                                                                               |
| Adresse des Initiatorportals | Die IP-Adresse des Initiator-Netzwerkportals                                                                                       |

7. Wenn Sie mit Ihren Eingaben zufrieden sind, klicken Sie auf **Verbinden**.

SnapCenter stellt die iSCSI-Sitzung her.

8. Wiederholen Sie diesen Vorgang, um für jedes Ziel eine Sitzung einzurichten.

## Erstellen Sie FC-verbundene oder iSCSI-verbundene LUNs oder Festplatten

Der Windows-Host sieht die LUNs auf Ihrem Speichersystem als virtuelle Datenträger. Sie können SnapCenter verwenden, um eine FC- oder iSCSI-verbundene LUN zu erstellen und zu konfigurieren.



Wenn Sie Datenträger außerhalb von SnapCenter erstellen und formatieren möchten, werden nur die Dateisysteme NTFS und CSVFS unterstützt.

### Bevor Sie beginnen

- Sie müssen auf Ihrem Speichersystem ein Volume für die LUN erstellt haben.

Das Volume sollte nur LUNs enthalten und nur LUNs, die mit SnapCenter erstellt wurden.



Sie können auf einem von SnapCenter erstellten Klonvolume keine LUN erstellen, es sei denn, der Klon wurde bereits aufgeteilt.

- Sie müssen den FC- oder iSCSI-Dienst auf dem Speichersystem gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem hergestellt haben.
- Das SnapCenter Plug-Ins-Paket für Windows darf nur auf dem Host installiert werden, auf dem Sie die Festplatte erstellen.

### Über diese Aufgabe

- Sie können eine LUN nicht mit mehr als einem Host verbinden, es sei denn, die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt.
- Wenn eine LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird, der CSV (Cluster Shared Volumes) verwendet, müssen Sie die Festplatte auf dem Host erstellen, dem die Clustergruppe gehört.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.
4. Klicken Sie auf **Neu**.

Der Assistent zum Erstellen von Datenträgern wird geöffnet.

5. Identifizieren Sie auf der Seite „LUN-Name“ die LUN:

| In diesem Bereich... | Machen Sie Folgendes...                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------|
| Speichersystem       | Wählen Sie die SVM für die LUN aus.                                                                          |
| LUN-Pfad             | Klicken Sie auf <b>Durchsuchen</b> , um den vollständigen Pfad des Ordners auszuwählen, der die LUN enthält. |
| LUN-Name             | Geben Sie den Namen der LUN ein.                                                                             |

| In diesem Bereich... | Machen Sie Folgendes...                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Clustergröße         | <p>Wählen Sie die LUN-Blockzuweisungsgröße für den Cluster aus.</p> <p>Die Clustergröße hängt vom Betriebssystem und den Anwendungen ab.</p> |
| LUN-Bezeichnung      | Geben Sie optional einen beschreibenden Text für die LUN ein.                                                                                |

6. Wählen Sie auf der Seite „Datenträgertyp“ den Datenträgertyp aus:

| Wählen...                               | Wenn...                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dedizierte Festplatte                   | <p>Auf die LUN kann nur von einem Host aus zugegriffen werden.</p> <p>Ignorieren Sie das Feld <b>Ressourcengruppe</b>.</p>                                                                                                                                                                                                  |
| Gemeinsam genutzte Festplatte           | <p>Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt.</p> <p>Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld <b>Ressourcengruppe</b> ein. Sie müssen die Festplatte nur auf einem Host im Failovercluster erstellen.</p>                                                        |
| Gemeinsam genutztes Clustervolume (CSV) | <p>Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt, der CSV verwendet.</p> <p>Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld <b>Ressourcengruppe</b> ein. Stellen Sie sicher, dass der Host, auf dem Sie die Festplatte erstellen, der Eigentümer der Clustergruppe ist.</p> |

7. Geben Sie auf der Seite „Laufwerkeigenschaften“ die Laufwerkeigenschaften an:

| Eigentum                           | Beschreibung                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Einhängepunkt automatisch zuweisen | <p>SnapCenter weist basierend auf dem Systemlaufwerk automatisch einen Volume-Mount-Punkt zu.</p> <p>Wenn Ihr Systemlaufwerk beispielsweise C: ist, erstellt die automatische Zuweisung einen Volume-Mount-Punkt unter Ihrem Laufwerk C: (C:\scmnt\). Die automatische Zuweisung wird für gemeinsam genutzte Datenträger nicht unterstützt.</p> |

| Eigentum                                                             | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Laufwerksbuchstaben zuweisen                                         | Hängen Sie die Festplatte in das Laufwerk ein, das Sie in der angrenzenden Dropdown-Liste auswählen.                                                                                                                                                                                                                                                                                                                              |
| Volume-Mount-Punkt verwenden                                         | <p>Hängen Sie die Festplatte in den Laufwerkspfad ein, den Sie im angrenzenden Feld angeben.</p> <p>Das Stammverzeichnis des Volume-Mount-Punkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.</p>                                                                                                                                                                                                                 |
| Weder Laufwerksbuchstaben noch Volume-Mount-Punkte zuweisen          | Wählen Sie diese Option, wenn Sie die Festplatte lieber manuell in Windows mounten möchten.                                                                                                                                                                                                                                                                                                                                       |
| LUN-Größe                                                            | <p>Geben Sie die LUN-Größe an; mindestens 150 MB.</p> <p>Wählen Sie in der angrenzenden Dropdown-Liste MB, GB oder TB aus.</p>                                                                                                                                                                                                                                                                                                    |
| Verwenden Sie Thin Provisioning für das Volume, das diese LUN hostet | <p>Führen Sie eine Thin-Provisioning-Bereitstellung für die LUN durch.</p> <p>Thin Provisioning weist nur so viel Speicherplatz zu, wie jeweils benötigt wird, sodass die LUN effizient auf die maximal verfügbare Kapazität anwachsen kann.</p> <p>Stellen Sie sicher, dass auf dem Volume genügend Speicherplatz für den gesamten LUN-Speicher verfügbar ist, den Sie voraussichtlich benötigen.</p>                            |
| Partitionstyp auswählen                                              | <p>Wählen Sie eine GPT-Partition für eine GUID-Partitionstabelle oder eine MBR-Partition für einen Master Boot Record.</p> <p>MBR-Partitionen können in Windows Server-Failoverclustern zu Ausrichtungsproblemen führen.</p> <div>  <p>UEFI-Partitionsdatenträger (Unified Extensible Firmware Interface) werden nicht unterstützt.</p> </div> |

8. Wählen Sie auf der Seite „LUN zuordnen“ den iSCSI- oder FC-Initiator auf dem Host aus:

| In diesem Bereich...     | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gastgeber                | <p>Doppelklicken Sie auf den Clustergruppennamen, um eine Dropdownliste mit den zum Cluster gehörenden Hosts anzuzeigen, und wählen Sie dann den Host für den Initiator aus.</p> <p>Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird.</p> |
| Host-Initiator auswählen | <p>Wählen Sie <b>Fibre Channel</b> oder <b>iSCSI</b> und wählen Sie dann den Initiator auf dem Host.</p> <p>Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit Multipath I/O (MPIO) verwenden.</p>                                                                                                   |

9. Geben Sie auf der Seite „Gruppentyp“ an, ob Sie der LUN eine vorhandene Igroup zuordnen oder eine neue Igroup erstellen möchten:

| Wählen...                                                                                        | Wenn...                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Neue Igroup für ausgewählte Initiatoren erstellen                                                | Sie möchten eine neue Igroup für die ausgewählten Initiatoren erstellen.                                                                                                                                                                                                                                                                      |
| Wählen Sie eine vorhandene Igroup oder geben Sie eine neue Igroup für ausgewählte Initiatoren an | <p>Sie möchten eine vorhandene Igroup für die ausgewählten Initiatoren angeben oder eine neue Igroup mit dem von Ihnen angegebenen Namen erstellen.</p> <p>Geben Sie den Igroup-Namen in das Feld <b>Igroup-Name</b> ein. Geben Sie die ersten Buchstaben des vorhandenen Igroup-Namens ein, um das Feld automatisch zu vervollständigen.</p> |

10. Überprüfen Sie auf der Seite „Zusammenfassung“ Ihre Auswahl und klicken Sie dann auf **Fertig**.

SnapCenter erstellt die LUN und verbindet sie mit dem angegebenen Laufwerk oder Laufwerkspfad auf dem Host.

## Ändern der Größe einer Festplatte

Sie können die Größe einer Festplatte vergrößern oder verkleinern, wenn sich die Anforderungen Ihres Speichersystems ändern.

## Über diese Aufgabe

- Für Thin Provisioning LUN wird die ONTAP LUN-Geometriegröße als maximale Größe angezeigt.
- Bei Thick Provisioning LUN wird die erweiterbare Größe (verfügbare Größe im Volume) als maximale Größe angezeigt.
- LUNs mit Partitionen im MBR-Stil haben eine Größenbeschränkung von 2 TB.

- LUNs mit Partitionen im GPT-Stil haben eine Speichersystemgrößenbeschränkung von 16 TB.
- Es ist eine gute Idee, vor der Größenänderung einer LUN einen Snapshot zu erstellen.
- Wenn Sie eine LUN aus einem Snapshot wiederherstellen müssen, der vor der Größenänderung der LUN erstellt wurde, passt SnapCenter die Größe der LUN automatisch an die Größe des Snapshots an.

Nach dem Wiederherstellungsvorgang müssen Daten, die der LUN nach der Größenänderung hinzugefügt wurden, aus einem Snapshot wiederhergestellt werden, der nach der Größenänderung erstellt wurde.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Host aus der Dropdown-Liste „Host“ aus.

Die Datenträger werden aufgelistet.

4. Wählen Sie die Festplatte aus, deren Größe Sie ändern möchten, und klicken Sie dann auf **Größe ändern**.
5. Verwenden Sie im Dialogfeld „Datenträgergröße ändern“ den Schieberegler, um die neue Größe des Datenträgers festzulegen, oder geben Sie die neue Größe in das Feld „Größe“ ein.



Wenn Sie die Größe manuell eingeben, müssen Sie außerhalb des Felds „Größe“ klicken, bevor die Schaltfläche „Verkleinern“ oder „Erweitern“ entsprechend aktiviert wird. Außerdem müssen Sie auf MB, GB oder TB klicken, um die Maßeinheit anzugeben.

6. Wenn Sie mit Ihren Eingaben zufrieden sind, klicken Sie je nach Bedarf auf **Verkleinern** oder **Erweitern**.

SnapCenter ändert die Größe der Festplatte.

## Verbinden einer Festplatte

Mit dem Assistenten „Datenträger verbinden“ können Sie eine vorhandene LUN mit einem Host verbinden oder eine getrennte LUN erneut verbinden.

### Bevor Sie beginnen

- Sie müssen den FC- oder iSCSI-Dienst auf dem Speichersystem gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem hergestellt haben.
- Sie können eine LUN nicht mit mehr als einem Host verbinden, es sei denn, die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt.
- Wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird, der CSV (Cluster Shared Volumes) verwendet, müssen Sie die Festplatte auf dem Host verbinden, dem die Clustergruppe gehört.
- Das Plug-in für Windows muss nur auf dem Host installiert werden, an den Sie die Festplatte anschließen.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

4. Klicken Sie auf **Verbinden**.

Der Assistent „Datenträger verbinden“ wird geöffnet.

5. Identifizieren Sie auf der Seite „LUN-Name“ die LUN, mit der eine Verbindung hergestellt werden soll:

| In diesem Bereich... | Machen Sie Folgendes...                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Speichersystem       | Wählen Sie die SVM für die LUN aus.                                                                                                   |
| LUN-Pfad             | Klicken Sie auf <b>Durchsuchen</b> , um den vollständigen Pfad des Volumes auszuwählen, das die LUN enthält.                          |
| LUN-Name             | Geben Sie den Namen der LUN ein.                                                                                                      |
| Clustergröße         | Wählen Sie die LUN-Blockzuweisungsgröße für den Cluster aus.<br><br>Die Clustergröße hängt vom Betriebssystem und den Anwendungen ab. |
| LUN-Bezeichnung      | Geben Sie optional einen beschreibenden Text für die LUN ein.                                                                         |

6. Wählen Sie auf der Seite „Datenträgertyp“ den Datenträgertyp aus:

| Wählen...                               | Wenn...                                                                                                                                                                                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dedizierte Festplatte                   | Auf die LUN kann nur von einem Host aus zugegriffen werden.                                                                                                                                                                                 |
| Gemeinsam genutzte Festplatte           | Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt.<br><br>Sie müssen die Festplatte nur mit einem Host im Failovercluster verbinden.                                                                         |
| Gemeinsam genutztes Clustervolume (CSV) | Die LUN wird von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt, der CSV verwendet.<br><br>Stellen Sie sicher, dass der Host, auf dem Sie eine Verbindung zur Festplatte herstellen, der Eigentümer der Clustergruppe ist. |

7. Geben Sie auf der Seite „Laufwerkeigenschaften“ die Laufwerkeigenschaften an:

| Eigentum                                                    | Beschreibung                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Automatische Zuweisung                                      | <p>Lassen Sie SnapCenter automatisch einen Volume-Mount-Punkt basierend auf dem Systemlaufwerk zuweisen.</p> <p>Wenn Ihr Systemlaufwerk beispielsweise C: ist, erstellt die automatische Zuweisungseigenschaft einen Volume-Mount-Punkt unter Ihrem Laufwerk C: (C:\scmnt\). Die Eigenschaft „Automatische Zuweisung“ wird für gemeinsam genutzte Datenträger nicht unterstützt.</p> |
| Laufwerksbuchstaben zuweisen                                | Hängen Sie die Festplatte in das Laufwerk ein, das Sie in der angrenzenden Dropdown-Liste auswählen.                                                                                                                                                                                                                                                                                 |
| Volume-Mount-Punkt verwenden                                | <p>Hängen Sie die Festplatte in den Laufwerkspfad ein, den Sie im angrenzenden Feld angeben.</p> <p>Das Stammverzeichnis des Volume-Mount-Punkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.</p>                                                                                                                                                                    |
| Weder Laufwerksbuchstaben noch Volume-Mount-Punkte zuweisen | Wählen Sie diese Option, wenn Sie die Festplatte lieber manuell in Windows mounten möchten.                                                                                                                                                                                                                                                                                          |

8. Wählen Sie auf der Seite „LUN zuordnen“ den iSCSI- oder FC-Initiator auf dem Host aus:

| In diesem Bereich...     | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gastgeber                | <p>Doppelklicken Sie auf den Clustergruppennamen, um eine Dropdown-Liste mit den zum Cluster gehörenden Hosts anzuzeigen. Wählen Sie dann den Host für den Initiator aus.</p> <p>Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird.</p> |
| Host-Initiator auswählen | <p>Wählen Sie <b>Fibre Channel</b> oder <b>iSCSI</b> und wählen Sie dann den Initiator auf dem Host.</p> <p>Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit MPIO verwenden.</p>                                                                                                                |

9. Geben Sie auf der Seite „Gruppentyp“ an, ob Sie der LUN eine vorhandene Igroup zuordnen oder eine neue Igroup erstellen möchten:

| Wählen...                                                                                        | Wenn...                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Neue igroup für ausgewählte Initiatoren erstellen                                                | Sie möchten eine neue Igroup für die ausgewählten Initiatoren erstellen.                                                                                                                                                                                                                                                              |
| Wählen Sie eine vorhandene Igroup oder geben Sie eine neue Igroup für ausgewählte Initiatoren an | <p>Sie möchten eine vorhandene Igroup für die ausgewählten Initiatoren angeben oder eine neue Igroup mit dem von Ihnen angegebenen Namen erstellen.</p> <p>Geben Sie den Igroup-Namen in das Feld <b>Igroup-Name</b> ein. Geben Sie die ersten Buchstaben des vorhandenen igroup-Namens ein, um das Feld automatisch auszufüllen.</p> |

10. Überprüfen Sie auf der Seite „Zusammenfassung“ Ihre Auswahl und klicken Sie auf „Fertig stellen“.

SnapCenter verbindet die LUN mit dem angegebenen Laufwerk oder Laufwerkspfad auf dem Host.

## Trennen einer Festplatte

Sie können eine LUN von einem Host trennen, ohne den Inhalt der LUN zu beeinträchtigen, mit einer Ausnahme: Wenn Sie einen Klon trennen, bevor er abgespalten wurde, verlieren Sie den Inhalt des Klons.

### Bevor Sie beginnen

- Stellen Sie sicher, dass die LUN von keiner Anwendung verwendet wird.
- Stellen Sie sicher, dass die LUN nicht mit einer Überwachungssoftware überwacht wird.
- Wenn die LUN gemeinsam genutzt wird, stellen Sie sicher, dass Sie die Cluster-Ressourcenabhängigkeiten von der LUN entfernen und überprüfen, ob alle Knoten im Cluster eingeschaltet sind, ordnungsgemäß funktionieren und für SnapCenter verfügbar sind.

### Über diese Aufgabe

Wenn Sie eine LUN in einem von SnapCenter erstellten FlexClone -Volume trennen und keine anderen LUNs auf dem Volume verbunden sind, löscht SnapCenter das Volume. Bevor die LUN getrennt wird, zeigt SnapCenter eine Warnmeldung an, dass das FlexClone Volume möglicherweise gelöscht wird.

Um das automatische Löschen des FlexClone -Volumes zu vermeiden, sollten Sie das Volume umbenennen, bevor Sie die letzte LUN trennen. Achten Sie beim Umbenennen des Datenträgers darauf, dass Sie mehrere Zeichen ändern und nicht nur das letzte Zeichen im Namen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

Die Datenträger werden aufgelistet.

4. Wählen Sie die Festplatte aus, die Sie trennen möchten, und klicken Sie dann auf **Trennen**.



5. Klicken Sie im Dialogfeld „Datenträger trennen“ auf **OK**.

SnapCenter trennt die Verbindung zur Festplatte.

## Löschen eines Datenträgers

Sie können eine Festplatte löschen, wenn Sie sie nicht mehr benötigen. Nachdem Sie eine Festplatte gelöscht haben, können Sie sie nicht wiederherstellen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Datenträger**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.

Die Datenträger werden aufgelistet.

4. Wählen Sie die Festplatte aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie im Dialogfeld „Datenträger löschen“ auf **OK**.

SnapCenter löscht die Festplatte.

## Erstellen und Verwalten von SMB-Freigaben

Zum Konfigurieren einer SMB3-Freigabe auf einer Storage Virtual Machine (SVM) können Sie entweder die SnapCenter -Benutzeroberfläche oder PowerShell-Cmdlets verwenden.

**Best Practice:** Die Verwendung der Cmdlets wird empfohlen, da Sie so die mit SnapCenter bereitgestellten Vorlagen nutzen können, um die Freigabekonfiguration zu automatisieren.

Die Vorlagen umfassen bewährte Methoden für die Volume- und Freigabekonfiguration. Sie finden die Vorlagen im Ordner „Templates“ im Installationsordner des SnapCenter Plug-ins-Pakets für Windows.



Wenn Sie sich dabei sicher fühlen, können Sie anhand der bereitgestellten Modelle Ihre eigenen Vorlagen erstellen. Sie sollten die Parameter in der Cmdlet-Dokumentation überprüfen, bevor Sie eine benutzerdefinierte Vorlage erstellen.

## Erstellen einer SMB-Freigabe

Sie können die SnapCenter Freigabenseite verwenden, um eine SMB3-Freigabe auf einer virtuellen Speichermaschine (SVM) zu erstellen.

Sie können SnapCenter nicht zum Sichern von Datenbanken auf SMB-Freigaben verwenden. Der SMB-Support ist nur auf die Bereitstellung beschränkt.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Freigaben**.

3. Wählen Sie die SVM aus der Dropdown-Liste **Storage Virtual Machine** aus.
4. Klicken Sie auf **Neu**.

Das Dialogfeld „Neue Freigabe“ wird geöffnet.

5. Definieren Sie im Dialogfeld „Neue Freigabe“ die Freigabe:

| In diesem Bereich... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Beschreibung         | Geben Sie einen beschreibenden Text für die Freigabe ein.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Freigabename         | <p>Geben Sie den Freigabennamen ein, beispielsweise „test_share“.</p> <p>Der Name, den Sie für die Freigabe eingeben, wird auch als Volumenname verwendet.</p> <p>Der Freigabename:</p> <ul style="list-style-type: none"> <li>• Muss eine UTF-8-Zeichenfolge sein.</li> <li>• Darf die folgenden Zeichen nicht enthalten: Steuerzeichen von 0x00 bis 0x1F (beide inklusive), 0x22 (doppelte Anführungszeichen) und die Sonderzeichen \ / [ ] : (vertical bar) &lt; &gt; + = ; , ?</li> </ul> |
| Pfad teilen          | <ul style="list-style-type: none"> <li>• Klicken Sie in das Feld, um einen neuen Dateisystempfad einzugeben, beispielsweise /.</li> <li>• Doppelklicken Sie in das Feld, um aus einer Liste vorhandener Dateisystempfade auszuwählen.</li> </ul>                                                                                                                                                                                                                                              |

6. Wenn Sie mit Ihren Eingaben zufrieden sind, klicken Sie auf **OK**.

SnapCenter erstellt die SMB-Freigabe auf der SVM.

## Löschen einer SMB-Freigabe

Sie können eine SMB-Freigabe löschen, wenn Sie sie nicht mehr benötigen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Freigaben**.
3. Klicken Sie auf der Seite „Freigaben“ in das Feld **Storage Virtual Machine**, um ein Dropdown-Menü mit einer Liste der verfügbaren Storage Virtual Machines (SVMs) anzuzeigen. Wählen Sie dann die SVM für die Freigabe aus, die Sie löschen möchten.
4. Wählen Sie aus der Liste der Freigaben auf der SVM die Freigabe aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.

5. Klicken Sie im Dialogfeld „Freigabe löschen“ auf **OK**.

SnapCenter löscht die SMB-Freigabe aus der SVM.

### **Speicherplatz auf dem Speichersystem freigeben**

Obwohl NTFS den verfügbaren Speicherplatz auf einer LUN verfolgt, wenn Dateien gelöscht oder geändert werden, meldet es die neuen Informationen nicht an das Speichersystem. Sie können das PowerShell-Cmdlet zur Speicherplatzrückgewinnung auf dem Plug-in für Windows-Host ausführen, um sicherzustellen, dass neu freigegebene Blöcke als im Speicher verfügbar markiert werden.

Wenn Sie das Cmdlet auf einem Remote-Plug-In-Host ausführen, müssen Sie das Cmdlet SnapCenterOpen-SMConnection ausgeführt haben, um eine Verbindung zum SnapCenter -Server zu öffnen.

### **Bevor Sie beginnen**

- Sie müssen sicherstellen, dass der Prozess zur Speicherplatzrückgewinnung abgeschlossen ist, bevor Sie einen Wiederherstellungsvorgang durchführen.
- Wenn die LUN von Hosts in einem Windows Server-Failovercluster gemeinsam genutzt wird, müssen Sie die Speicherplatzrückgewinnung auf dem Host durchführen, dem die Clustergruppe gehört.
- Für eine optimale Speicherleistung sollten Sie die Speicherplatzrückgewinnung so oft wie möglich durchführen.

Sie sollten sicherstellen, dass das gesamte NTFS-Dateisystem gescannt wurde.

### **Über diese Aufgabe**

- Die Speicherplatzrückgewinnung ist zeitaufwändig und CPU-intensiv. Daher ist es normalerweise am besten, den Vorgang auszuführen, wenn die Auslastung des Speichersystems und des Windows-Hosts gering ist.
- Durch die Speicherplatzrückgewinnung wird fast der gesamte verfügbare Speicherplatz zurückgewonnen, jedoch nicht 100 Prozent.
- Sie sollten die Festplattendefragmentierung nicht gleichzeitig mit der Speicherplatzrückgewinnung ausführen.

Dies kann den Wiederherstellungsprozess verlangsamen.

### **Schritt**

Geben Sie in der PowerShell-Eingabeaufforderung des Anwendungsservers den folgenden Befehl ein:

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive\_path ist der Laufwerkspfad, der der LUN zugeordnet ist.

### **Bereitstellen von Speicher mithilfe von PowerShell-Cmdlets**

Wenn Sie die SnapCenter -GUI nicht zum Ausführen von Hostbereitstellungs- und Speicherplatzrückgewinnungsaufträgen verwenden möchten, können Sie die PowerShell-Cmdlets verwenden. Sie können Cmdlets direkt verwenden oder sie zu Skripten

hinzufügen.

Wenn Sie die Cmdlets auf einem Remote-Plug-In-Host ausführen, müssen Sie das SnapCenter Open-SMConnection-Cmdlet ausführen, um eine Verbindung zum SnapCenter -Server zu öffnen.

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"](#) .

Wenn SnapCenter PowerShell-Cmdlets aufgrund der Entfernung von SnapDrive für Windows vom Server beschädigt sind, lesen Sie ["SnapCenter -Cmdlets funktionieren nicht mehr, wenn SnapDrive für Windows deinstalliert wird"](#) .

## Bereitstellen von Speicher in VMware-Umgebungen

Sie können das SnapCenter Plug-in für Microsoft Windows in VMware-Umgebungen verwenden, um LUNs zu erstellen und zu verwalten und Snapshots zu verwalten.

### Unterstützte VMware-Gastbetriebssystemplattformen

- Unterstützte Versionen von Windows Server
- Microsoft-Clusterkonfigurationen

Unterstützung für bis zu maximal 16 Knoten auf VMware bei Verwendung des Microsoft iSCSI Software Initiator oder bis zu zwei Knoten bei Verwendung von FC

- RDM-LUNs

Unterstützung für maximal 56 RDM-LUNs mit vier LSI Logic SCSI-Controllern für normales RDMS oder 42 RDM-LUNs mit drei LSI Logic SCSI-Controllern auf einem VMware VM MSCS Box-to-Box-Plug-in für Windows-Konfiguration

Unterstützt VMware ParaVirtual SCSI Controller. Auf RDM-Festplatten können 256 Festplatten unterstützt werden.

Aktuelle Informationen zu unterstützten Versionen finden Sie unter ["NetApp Interoperabilitätsmatrix-Tool"](#) .

### Einschränkungen im Zusammenhang mit VMware ESXi-Servern

- Die Installation des Plug-ins für Windows auf einem Microsoft-Cluster auf virtuellen Maschinen mit ESXi-Anmeldeinformationen wird nicht unterstützt.

Sie sollten Ihre vCenter-Anmeldeinformationen verwenden, wenn Sie das Plug-in für Windows auf virtuellen Maschinen im Cluster installieren.

- Alle Clusterknoten müssen dieselbe Ziel-ID (auf dem virtuellen SCSI-Adapter) für dieselbe Clusterfestplatte verwenden.
- Wenn Sie eine RDM-LUN außerhalb des Plug-ins für Windows erstellen, müssen Sie den Plug-in-Dienst neu starten, damit er die neu erstellte Festplatte erkennt.
- Sie können iSCSI- und FC-Initiatoren nicht gleichzeitig auf einem VMware-Gastbetriebssystem verwenden.

## Für SnapCenter RDM-Vorgänge erforderliche Mindestberechtigungen für vCenter

Sie sollten über die folgenden vCenter-Berechtigungen auf dem Host verfügen, um RDM-Vorgänge in einem Gastbetriebssystem durchzuführen:

- Datenspeicher: Datei entfernen
- Host: Konfiguration > Speicherpartitionskonfiguration
- Virtuelle Maschine: Konfiguration

Sie müssen diese Berechtigungen einer Rolle auf der Virtual Center Server-Ebene zuweisen. Die Rolle, der Sie diese Berechtigungen zuweisen, kann keinem Benutzer ohne Root-Berechtigungen zugewiesen werden.

Nachdem Sie diese Berechtigungen zugewiesen haben, können Sie das Plug-in für Windows auf dem Gastbetriebssystem installieren.

### Verwalten von FC RDM LUNs in einem Microsoft-Cluster

Sie können das Plug-in für Windows verwenden, um einen Microsoft-Cluster mithilfe von FC RDM LUNs zu verwalten. Sie müssen jedoch zuerst das gemeinsam genutzte RDM-Quorum und den gemeinsam genutzten Speicher außerhalb des Plug-ins erstellen und dann die Festplatten zu den virtuellen Maschinen im Cluster hinzufügen.

Ab ESXi 5.5 können Sie auch ESX iSCSI- und FCoE-Hardware zur Verwaltung eines Microsoft-Clusters verwenden. Das Plug-in für Windows umfasst sofort einsatzbereite Unterstützung für Microsoft-Cluster.

### Anforderungen

Das Plug-in für Windows bietet Unterstützung für Microsoft-Cluster mithilfe von FC RDM LUNs auf zwei verschiedenen virtuellen Maschinen, die zu zwei verschiedenen ESX- oder ESXi-Servern gehören (auch als Cluster über Boxen bezeichnet), wenn Sie bestimmte Konfigurationsanforderungen erfüllen.

- Auf den virtuellen Maschinen (VMs) muss dieselbe Windows Server-Version ausgeführt werden.
- Die ESX- oder ESXi-Serverversionen müssen für jeden übergeordneten VMware-Host identisch sein.
- Jeder übergeordnete Host muss über mindestens zwei Netzwerkadapter verfügen.
- Es muss mindestens ein von den beiden ESX- oder ESXi-Servern gemeinsam genutzter VMware Virtual Machine File System (VMFS)-Datenspeicher vorhanden sein.
- VMware empfiehlt, den gemeinsam genutzten Datenspeicher auf einem FC-SAN zu erstellen.

Bei Bedarf kann der gemeinsame Datenspeicher auch über iSCSI erstellt werden.

- Die gemeinsam genutzte RDM-LUN muss sich im physischen Kompatibilitätsmodus befinden.
- Die gemeinsam genutzte RDM-LUN muss manuell außerhalb des Plug-ins für Windows erstellt werden.

Sie können virtuelle Datenträger nicht für gemeinsam genutzten Speicher verwenden.

- Auf jeder virtuellen Maschine im Cluster muss im physischen Kompatibilitätsmodus ein SCSI-Controller konfiguriert werden:

Windows Server 2008 R2 erfordert, dass Sie den LSI Logic SAS SCSI-Controller auf jeder virtuellen Maschine konfigurieren. Gemeinsam genutzte LUNs können den vorhandenen LSI Logic SAS-Controller nicht verwenden, wenn nur einer seines Typs vorhanden ist und dieser bereits an das Laufwerk C: angeschlossen ist.

SCSI-Controller vom Typ „Paravirtual“ werden auf VMware Microsoft-Clustern nicht unterstützt.



Wenn Sie einen SCSI-Controller zu einer freigegebenen LUN auf einer virtuellen Maschine im physischen Kompatibilitätsmodus hinzufügen, müssen Sie im VMware Infrastructure Client die Option **Raw Device Mappings** (RDM) und nicht die Option **Neue Festplatte erstellen** auswählen.

- Microsoft-Cluster virtueller Maschinen können nicht Teil eines VMware-Clusters sein.
- Sie müssen vCenter-Anmeldeinformationen und keine ESX- oder ESXi-Anmeldeinformationen verwenden, wenn Sie das Plug-in für Windows auf virtuellen Maschinen installieren, die zu einem Microsoft-Cluster gehören.
- Das Plug-in für Windows kann keine einzelne igroup mit Initiatoren von mehreren Hosts erstellen.

Die igroup, die die Initiatoren aller ESXi-Hosts enthält, muss auf dem Speichercontroller erstellt werden, bevor die RDM-LUNs erstellt werden, die als gemeinsam genutzte Cluster-Festplatten verwendet werden.

- Stellen Sie sicher, dass Sie mithilfe eines FC-Initiators eine RDM-LUN auf ESXi 5.0 erstellen.

Wenn Sie eine RDM-LUN erstellen, wird mit ALUA eine Initiatorgruppe erstellt.

## Einschränkungen

Das Plug-in für Windows unterstützt Microsoft-Cluster mithilfe von FC/iSCSI RDM LUNs auf verschiedenen virtuellen Maschinen, die zu verschiedenen ESX- oder ESXi-Servern gehören.



Diese Funktion wird in Versionen vor ESX 5.5i nicht unterstützt.

- Das Plug-in für Windows unterstützt keine Cluster auf ESX iSCSI- und NFS-Datenspeichern.
- Das Plug-in für Windows unterstützt keine gemischten Initiatoren in einer Clusterumgebung.

Initiatoren müssen entweder FC oder Microsoft iSCSI sein, aber nicht beides.

- ESX iSCSI-Initiatoren und HBAs werden auf gemeinsam genutzten Datenträgern in einem Microsoft-Cluster nicht unterstützt.
- Das Plug-in für Windows unterstützt keine Migration virtueller Maschinen mit vMotion, wenn die virtuelle Maschine Teil eines Microsoft-Clusters ist.
- Das Plug-in für Windows unterstützt MPIO auf virtuellen Maschinen in einem Microsoft-Cluster nicht.

## Erstellen einer freigegebenen FC RDM LUN

Bevor Sie FC RDM LUNs verwenden können, um Speicher zwischen Knoten in einem Microsoft-Cluster gemeinsam zu nutzen, müssen Sie zunächst die gemeinsam genutzte Quorum-Festplatte und die gemeinsam genutzte Speicherfestplatte erstellen und sie dann zu beiden virtuellen Maschinen im Cluster hinzufügen.

Die freigegebene Festplatte wird nicht mit dem Plug-in für Windows erstellt. Sie sollten die gemeinsam genutzte LUN erstellen und dann zu jeder virtuellen Maschine im Cluster hinzufügen. Weitere Informationen finden Sie unter ["Clustern virtueller Maschinen über physische Hosts"](#).

## Hinzufügen von Controller-basierten Lizenzen für SnapCenter Standard

Wenn Sie FAS, AFF oder ASA Speichercontroller verwenden, ist eine Controller-basierte Lizenz für SnapCenter Standard erforderlich.

Die Controller-basierte Lizenz weist die folgenden Merkmale auf:

- SnapCenter Standard-Berechtigung im Kauf von Premium oder Flash Bundle enthalten (nicht im Basispaket)
- Unbegrenzte Speichernutzung
- Wird mithilfe des ONTAP System Manager oder der ONTAP CLI direkt zum FAS, AFF oder ASA -Speichercontroller hinzugefügt.



Für die Controller-basierten Lizenzen von SnapCenter geben Sie in der SnapCenter -Benutzeroberfläche keine Lizenzinformationen ein.

- An die Seriennummer des Controllers gebunden

Informationen zu den erforderlichen Lizenzen finden Sie unter "[SnapCenter -Lizenzen](#)".

### Schritt 1: Überprüfen Sie, ob die SnapManager Suite-Lizenz installiert ist

Sie können die SnapCenter Benutzeroberfläche verwenden, um zu überprüfen, ob eine SnapManager Suite-Lizenz auf FAS, AFF oder ASA Primärspeichersystemen installiert ist, und um festzustellen, welche Systeme Lizenzen benötigen. SnapManager Suite-Lizenzen gelten nur für FAS, AFF und ASA -SVMs oder Cluster auf primären Speichersystemen.



Wenn Sie bereits über eine SnapManager Suite-Lizenz auf Ihrem Controller verfügen, stellt SnapCenter automatisch die Berechtigung für die Standard-Controller-basierte Lizenz bereit. Die Bezeichnungen SnapManagerSuite-Lizenz und Controller-basierte SnapCenter Standard-Lizenz werden synonym verwendet, beziehen sich jedoch auf dieselbe Lizenz.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Speichersysteme** aus.
2. Wählen Sie auf der Seite „Speichersysteme“ im Dropdown-Menü „Typ“ aus, ob alle hinzugefügten SVMs oder Cluster angezeigt werden sollen:
  - Um alle hinzugefügten SVMs anzuzeigen, wählen Sie \* ONTAP SVMs\*.
  - Um alle hinzugefügten Cluster anzuzeigen, wählen Sie \* ONTAP -Cluster\*.

Wenn Sie den Clusternamen auswählen, werden alle SVMs, die Teil des Clusters sind, im Abschnitt „Storage Virtual Machines“ angezeigt.

3. Suchen Sie in der Liste „Speicherverbindungen“ die Spalte „Controller-Lizenz“.

In der Spalte „Controller-Lizenz“ wird der folgende Status angezeigt:

◦



zeigt an, dass eine SnapManager Suite-Lizenz auf einem FAS, AFF oder ASA Primärspeichersystem installiert ist.

◦



zeigt an, dass auf einem FAS, AFF oder ASA Primärspeichersystem keine SnapManager Suite-Lizenz installiert ist.

- Nicht anwendbar bedeutet, dass eine SnapManager Suite-Lizenz nicht anwendbar ist, da sich der Speichercontroller auf Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select oder sekundäre Speicherplattformen befindet.

## Schritt 2: Identifizieren der auf dem Controller installierten Lizenzen

Sie können die ONTAP -Befehlszeile verwenden, um alle auf Ihrem Controller installierten Lizenzen anzuzeigen. Sie sollten Clusteradministrator auf dem FAS, AFF oder ASA System sein.



Der Controller zeigt die Controller-basierte Lizenz von SnapCenter Standard als SnapManagerSuite-Lizenz an.

### Schritte

1. Melden Sie sich über die ONTAP -Befehlszeile beim NetApp -Controller an.
2. Geben Sie den Befehl „license show“ ein und sehen Sie sich dann die Ausgabe an, um zu sehen, ob die SnapManagerSuite-Lizenz installiert ist.

### Beispielausgabe

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package          Type      Description              Expiration
-----
Base             site     Cluster Base License    -

Serial Number: 1-81-000000000000000000000000xx
Owner: cluster1-01
Package          Type      Description              Expiration
-----
NFS              license   NFS License             -
CIFS             license   CIFS License            -
iSCSI            license   iSCSI License           -
FCP              license   FCP License             -
SnapRestore      license   SnapRestore License     -
SnapMirror       license   SnapMirror License      -
FlexClone        license   FlexClone License       -
SnapVault        license   SnapVault License       -
SnapManagerSuite license   SnapManagerSuite License -
```

Im Beispiel ist die SnapManagerSuite-Lizenz installiert, daher ist keine zusätzliche SnapCenter



-Lizenzierungsaktion erforderlich.

### **Schritt 3: Rufen Sie die Seriennummer des Controllers ab**

Rufen Sie die Seriennummer des Controllers mithilfe der ONTAP -Befehlszeile ab. Sie müssen Clusteradministrator auf dem FAS, AFF oder ASA -System sein, um Ihre Controller-basierte Lizenzseriennummer zu erhalten.

#### **Schritte**

1. Melden Sie sich über die ONTAP -Befehlszeile beim Controller an.
2. Geben Sie den Befehl „system show -instance“ ein und überprüfen Sie dann die Ausgabe, um die Seriennummer des Controllers zu finden.

## Beispielausgabe

```
cluster1::> system show -instance
```

```
Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Notieren Sie die Seriennummern.

### Schritt 4: Seriennummer der Controller-basierten Lizenz abrufen

Wenn Sie FAS, ASA oder AFF -Speicher verwenden, können Sie die Controller-basierte Lizenz für SnapCenter von der NetApp -Support-Site abrufen, bevor Sie sie über die ONTAP -Befehlszeile installieren.

#### Bevor Sie beginnen

- Sie sollten über gültige Anmeldeinformationen für die NetApp -Support-Site verfügen.

Wenn Sie keine gültigen Anmeldeinformationen eingeben, gibt das System keine Informationen zu Ihrer

Suche zurück.

- Sie sollten die Seriennummer des Controllers haben.

### Schritte

1. Melden Sie sich an bei ["NetApp Support Site"](#) .
2. Navigieren Sie zu **Systeme > Softwarelizenzen**.
3. Stellen Sie im Bereich „Auswahlkriterien“ sicher, dass die Seriennummer (auf der Rückseite des Geräts) ausgewählt ist, geben Sie die Seriennummer des Controllers ein und wählen Sie dann **Los!**.

Software Licenses

Selection Criteria

Choose a method by which to search

► Serial Number (located on back of unit) ▾ Enter Value:  Go!

Enter the Cluster Serial Number value without dashes..

- OR -

► Show Me All: Serial Numbers with Licenses ▾ For Company:  Go!

Es wird eine Liste der Lizenzen für den angegebenen Controller angezeigt.

4. Suchen und notieren Sie die Lizenz für SnapCenter Standard oder SnapManagerSuite.

### Schritt 5: Controllerbasierte Lizenz hinzufügen

Sie können die ONTAP Befehlszeile verwenden, um eine auf einem SnapCenter -Controller basierende Lizenz hinzuzufügen, wenn Sie FAS, AFF oder ASA Systeme verwenden und über eine SnapCenter Standard- oder SnapManagerSuite-Lizenz verfügen.

#### Bevor Sie beginnen

- Sie sollten Clusteradministrator auf dem FAS, AFF oder ASA System sein.
- Sie sollten über die Lizenz SnapCenter Standard oder SnapManagerSuite verfügen.

#### Informationen zu diesem Vorgang

Wenn Sie SnapCenter auf Testbasis mit FAS, AFF oder ASA -Speicher installieren möchten, können Sie eine Evaluierungslizenz für das Premium Bundle erwerben und auf Ihrem Controller installieren.

Wenn Sie SnapCenter testweise installieren möchten, sollten Sie sich an Ihren Vertriebsmitarbeiter wenden, um eine Evaluierungslizenz für das Premium Bundle zur Installation auf Ihrem Controller zu erhalten.

### Schritte

1. Melden Sie sich über die ONTAP -Befehlszeile beim NetApp -Cluster an.
2. Fügen Sie den SnapManagerSuite-Lizenzschlüssel hinzu:

```
system license add -license-code license_key
```

Dieser Befehl ist auf der Administratorberechtigungsebene verfügbar.

3. Stellen Sie sicher, dass die SnapManagerSuite-Lizenz installiert ist:

```
license show
```

## Schritt 6: Entfernen Sie die Testlizenz

Wenn Sie eine Controller-basierte SnapCenter Standard-Lizenz verwenden und die kapazitätsbasierte Testlizenz (Seriennummer endet mit „50“) entfernen müssen, sollten Sie MySQL-Befehle verwenden, um die Testlizenz manuell zu entfernen. Die Testlizenz kann nicht über die SnapCenter Benutzeroberfläche gelöscht werden.



Das manuelle Entfernen einer Testlizenz ist nur erforderlich, wenn Sie eine Controller-basierte Lizenz für SnapCenter Standard verwenden.

### Schritte

1. Öffnen Sie auf dem SnapCenter -Server ein PowerShell-Fenster, um das MySQL-Kennwort zurückzusetzen.
  - a. Führen Sie das Cmdlet `Open-SmConnection` aus, um eine Verbindung mit dem SnapCenter -Server für ein SnapCenterAdmin-Konto herzustellen.
  - b. Führen Sie `„Set-SmRepositoryPassword“` aus, um das MySQL-Passwort zurückzusetzen.

Informationen zu den Cmdlets finden Sie unter ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

2. Öffnen Sie die Eingabeaufforderung und führen Sie `mysql -u root -p` aus, um sich bei MySQL anzumelden.

MySQL fordert Sie zur Eingabe des Kennworts auf. Geben Sie die Anmeldeinformationen ein, die Sie beim Zurücksetzen des Kennworts angegeben haben.

3. Entfernen Sie die Testlizenz aus der Datenbank:

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

## Konfigurieren der Hochverfügbarkeit

### Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit

Um Hochverfügbarkeit (HA) in SnapCenter unter Windows oder Linux zu unterstützen, können Sie den F5-Lastenausgleich installieren. F5 ermöglicht dem SnapCenter Server die Unterstützung von Aktiv-Passiv-Konfigurationen auf bis zu zwei Hosts am selben Standort. Um den F5 Load Balancer in SnapCenter zu verwenden, sollten Sie die SnapCenter -Server und den F5 Load Balancer konfigurieren.

Sie können auch Network Load Balancing (NLB) konfigurieren, um SnapCenter High Availability einzurichten. Für eine hohe Verfügbarkeit sollten Sie NLB außerhalb der SnapCenter -Installation manuell konfigurieren.

Für Cloudumgebungen können Sie Hochverfügbarkeit entweder mit Amazon Web Services (AWS) Elastic Load Balancing (ELB) oder Azure Load Balancer konfigurieren.

## Konfigurieren der Hochverfügbarkeit mit F5

Anweisungen zum Konfigurieren von SnapCenter -Servern für hohe Verfügbarkeit mit F5 Load Balancer finden Sie unter ["So konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit mit F5 Load Balancer"](#) .

Sie müssen Mitglied der lokalen Administratorgruppe auf den SnapCenter -Servern sein (und Ihnen muss zusätzlich die Rolle „SnapCenterAdmin“ zugewiesen sein), um die folgenden Cmdlets zum Hinzufügen und Entfernen von F5-Clustern verwenden zu können:

- Add-SmServerCluster
- SmServer hinzufügen
- Entfernen-SmServerCluster

Weitere Informationen finden Sie unter ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

### Weitere Informationen

- Nachdem Sie SnapCenter für hohe Verfügbarkeit installiert und konfiguriert haben, bearbeiten Sie die SnapCenter Desktopverknüpfung so, dass sie auf die IP des F5-Clusters verweist.
- Wenn ein Failover zwischen SnapCenter -Servern auftritt und auch eine SnapCenter -Sitzung vorhanden ist, müssen Sie den Browser schließen und sich erneut bei SnapCenter anmelden.
- Wenn Sie beim Einrichten des Lastenausgleichs (NLB oder F5) einen Host hinzufügen, der teilweise vom NLB- oder F5-Host aufgelöst wird, und der SnapCenter Host diesen Host nicht erreichen kann, wechselt die SnapCenter Hostseite häufig zwischen dem Status „Hosts ausgefallen“ und „Hosts ausgeführt“. Um dieses Problem zu beheben, sollten Sie sicherstellen, dass beide SnapCenter -Hosts den Host im NLB- oder F5-Host auflösen können.
- SnapCenter -Befehle für MFA-Einstellungen sollten auf allen Hosts ausgeführt werden. Die Konfiguration der vertrauenden Seite sollte auf dem Active Directory Federation Services (AD FS)-Server mithilfe der F5-Clusterdetails erfolgen. Der Zugriff auf die SnapCenter Benutzeroberfläche auf Hostebene wird blockiert, nachdem MFA aktiviert wurde.
- Während des Failovers werden die Audit-Protokolleinstellungen nicht auf dem zweiten Host angezeigt. Daher sollten Sie die Audit-Protokolleinstellungen auf dem passiven F5-Host manuell wiederholen, wenn dieser aktiv wird.

## Konfigurieren Sie Hochverfügbarkeit mithilfe des Netzwerklastenausgleichs (NLB).

Sie können den Netzwerklastenausgleich (NLB) konfigurieren, um SnapCenter High Availability einzurichten. Für eine hohe Verfügbarkeit sollten Sie NLB außerhalb der SnapCenter -Installation manuell konfigurieren.

Informationen zum Konfigurieren des Netzwerklastenausgleichs (NLB) mit SnapCenter finden Sie unter ["So konfigurieren Sie NLB mit SnapCenter"](#) .

## Konfigurieren Sie Hochverfügbarkeit mit AWS Elastic Load Balancing (ELB).

Sie können eine SnapCenter -Umgebung mit hoher Verfügbarkeit in Amazon Web Services (AWS) konfigurieren, indem Sie zwei SnapCenter -Server in separaten Verfügbarkeitszonen (AZs) einrichten und sie für automatisches Failover konfigurieren. Die Architektur umfasst virtuelle private IP-Adressen, Routing-Tabellen und Synchronisierung zwischen aktiven und Standby-MySQL-Datenbanken.

### Schritte

1. Konfigurieren Sie die virtuelle private Overlay-IP in AWS. Weitere Informationen finden Sie unter ["Konfigurieren der virtuellen privaten Overlay-IP"](#) .

## 2. Vorbereiten Ihres Windows-Hosts

- a. Erzwingen, dass IPv4 gegenüber IPv6 priorisiert wird:
  - Speicherort: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
  - Schlüssel: DisabledComponents
  - Typ: REG\_DWORD
  - Wert: 0x20
- b. Stellen Sie sicher, dass die vollqualifizierten Domännennamen über DNS oder über die lokale Hostkonfiguration in die IPv4-Adressen aufgelöst werden können.
- c. Stellen Sie sicher, dass Sie keinen Systemproxy konfiguriert haben.
- d. Stellen Sie sicher, dass das Administratorkennwort auf beiden Windows-Servern identisch ist, wenn Sie ein Setup ohne Active Directory verwenden und sich die Server nicht in derselben Domäne befinden.
- e. Fügen Sie auf beiden Windows-Servern eine virtuelle IP hinzu.

## 3. Erstellen Sie den SnapCenter Cluster.

- a. Starten Sie Powershell und stellen Sie eine Verbindung zu SnapCenter her.  
`Open-SmConnection`
- b. Erstellen Sie den Cluster.  
`Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
- c. Fügen Sie den sekundären Server hinzu.  
`Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
- d. Holen Sie sich die Details zur Hochverfügbarkeit.  
`Get-SmServerConfig`

## 4. Erstellen Sie die Lambda-Funktion, um die Routing-Tabelle anzupassen, falls der virtuelle private IP-Endpunkt nicht verfügbar ist, überwacht von AWS CloudWatch. Weitere Informationen finden Sie unter ["Erstellen einer Lambda-Funktion"](#).

## 5. Erstellen Sie einen Monitor in CloudWatch, um die Verfügbarkeit des SnapCenter -Endpunkts zu überwachen. Ein Alarm wird so konfiguriert, dass er eine Lambda-Funktion auslöst, wenn der Endpunkt nicht erreichbar ist. Die Lambda-Funktion passt die Routing-Tabelle an, um den Datenverkehr zum aktiven SnapCenter -Server umzuleiten. Weitere Informationen finden Sie unter ["Erstellen Sie synthetische Kanarienvögel"](#).

## 6. Implementieren Sie einen Workflow mithilfe einer Schrittfunktion als Alternative zur CloudWatch-Überwachung, um kürzere Failover-Zeiten zu ermöglichen. Der Workflow umfasst eine Lambda-Testfunktion zum Testen der SnapCenter -URL, eine DynamoDB-Tabelle zum Speichern der Fehleranzahl und die Step-Funktion selbst.

- a. Verwenden Sie eine Lambda-Funktion zum Prüfen der SnapCenter -URL. Weitere Informationen finden Sie unter ["Erstellen einer Lambda-Funktion"](#).
- b. Erstellen Sie eine DynamoDB-Tabelle zum Speichern der Fehleranzahl zwischen zwei Step Function-Iterationen. Weitere Informationen finden Sie unter ["Erste Schritte mit DynamoDB-Tabellen"](#).
- c. Erstellen Sie die Schrittfunktion. Weitere Informationen finden Sie unter ["Step Function-Dokumentation"](#).

- d. Testen Sie einen einzelnen Schritt.
- e. Testen Sie die komplette Funktion.
- f. Erstellen Sie eine IAM-Rolle und passen Sie die Berechtigungen an, um die Lambda-Funktion ausführen zu dürfen.
- g. Erstellen Sie einen Zeitplan zum Auslösen der Step-Funktion. Weitere Informationen finden Sie unter ["Verwenden des Amazon EventBridge Scheduler zum Starten einer Step Function"](#) .

### Konfigurieren der Hochverfügbarkeit mit Azure Load Balancer

Sie können eine SnapCenter Umgebung mit hoher Verfügbarkeit mithilfe des Azure Load Balancers konfigurieren.

#### Schritte

1. Erstellen Sie mithilfe des Azure-Portals virtuelle Computer in einer Skalierungsgruppe. Mit dem Azure-VM-Skalierungssatz können Sie eine Gruppe von virtuellen Maschinen mit Lastenausgleich erstellen und verwalten. Die Anzahl der Instanzen virtueller Maschinen kann je nach Bedarf oder nach einem festgelegten Zeitplan automatisch erhöht oder verringert werden. Weitere Informationen finden Sie unter ["Erstellen virtueller Computer in einer Skalierungsgruppe mithilfe des Azure-Portals"](#) .
2. Melden Sie sich nach der Konfiguration der virtuellen Maschinen bei jeder virtuellen Maschine im VM-Set an und installieren Sie SnapCenter Server auf beiden Knoten.
3. Erstellen Sie den Cluster auf Host 1.  

```
Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
```
4. Fügen Sie den sekundären Server hinzu.  

```
Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
```
5. Erhalten Sie die Details zur Hochverfügbarkeit.  

```
Get-SmServerConfig
```
6. Erstellen Sie bei Bedarf den sekundären Host neu.  

```
Set-SmRepositoryConfig -RebuildSlave -Verbose
```
7. Failover zum zweiten Host.  

```
Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
```

== Wechseln Sie von NLB zu F5 für hohe Verfügbarkeit

Sie können Ihre SnapCenter HA-Konfiguration von Network Load Balancing (NLB) ändern, um F5 Load Balancer zu verwenden.

#### Schritte

1. Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit mit F5. ["Mehr erfahren"](#) .
2. Starten Sie PowerShell auf dem SnapCenter Server-Host.
3. Starten Sie eine Sitzung mit dem Cmdlet „Open-SmConnection“ und geben Sie dann Ihre Anmeldeinformationen ein.
4. Aktualisieren Sie den SnapCenter -Server mithilfe des Cmdlets „Update-SmServerCluster“, sodass er auf die IP-Adresse des F5-Clusters verweist.

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"](#) .

## Hohe Verfügbarkeit für das SnapCenter MySQL-Repository

Die MySQL-Replikation ist eine Funktion des MySQL-Servers, mit der Sie Daten von einem MySQL-Datenbankserver (Master) auf einen anderen MySQL-Datenbankserver (Slave) replizieren können. SnapCenter unterstützt die MySQL-Replikation für hohe Verfügbarkeit nur auf zwei Knoten mit aktiviertem Netzwerklastenausgleich (NLB).

SnapCenter führt Lese- oder Schreibvorgänge am Master-Repository aus und leitet seine Verbindung zum Slave-Repository um, wenn im Master-Repository ein Fehler auftritt. Das Slave-Repository wird dann zum Master-Repository. SnapCenter unterstützt auch die umgekehrte Replikation, die nur während eines Failovers aktiviert wird.

Wenn Sie die MySQL-Hochverfügbarkeitsfunktion (HA) verwenden möchten, müssen Sie Network Load Balancer (NLB) auf dem ersten Knoten konfigurieren. Das MySQL-Repository wird im Rahmen der Installation auf diesem Knoten installiert. Während Sie SnapCenter auf dem zweiten Knoten installieren, müssen Sie sich mit F5 des ersten Knotens verbinden und eine Kopie des MySQL-Repositorys auf dem zweiten Knoten erstellen.

SnapCenter bietet die PowerShell-Cmdlets *Get-SmRepositoryConfig* und *Set-SmRepositoryConfig* zur Verwaltung der MySQL-Replikation.

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"](#) .

Sie müssen sich der Einschränkungen im Zusammenhang mit der MySQL HA-Funktion bewusst sein:

- NLB und MySQL HA werden über zwei Knoten hinaus nicht unterstützt.
- Der Wechsel von einer eigenständigen SnapCenter -Installation zu einer NLB-Installation oder umgekehrt sowie der Wechsel von einem eigenständigen MySQL-Setup zu MySQL HA werden nicht unterstützt.
- Automatisches Failover wird nicht unterstützt, wenn die Daten des Slave-Repositorys nicht mit den Daten des Master-Repositorys synchronisiert sind.

Sie können ein erzwungenes Failover mithilfe des Cmdlets *Set-SmRepositoryConfig* initiieren.

- Wenn ein Failover eingeleitet wird, können laufende Jobs fehlschlagen.

Wenn ein Failover auftritt, weil der MySQL-Server oder der SnapCenter Server ausgefallen ist, können alle ausgeführten Jobs fehlschlagen. Nach dem Failover auf den zweiten Knoten werden alle nachfolgenden Jobs erfolgreich ausgeführt.

Informationen zum Konfigurieren von Hochverfügbarkeit finden Sie unter ["So konfigurieren Sie NLB und ARR mit SnapCenter"](#) .

## Konfigurieren der rollenbasierten Zugriffssteuerung (RBAC)



## Erstellen einer Rolle

Zusätzlich zur Verwendung der vorhandenen SnapCenter -Rollen können Sie Ihre eigenen Rollen erstellen und die Berechtigungen anpassen.

Um eigene Rollen zu erstellen, ist eine Anmeldung mit der Rolle „SnapCenterAdmin“ erforderlich.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Rollen**.
3. Klicken .
4. Geben Sie einen Namen und eine Beschreibung für die neue Rolle an.



In Benutzernamen und Gruppennamen dürfen nur die folgenden Sonderzeichen verwendet werden: Leerzeichen ( ), Bindestrich (-), Unterstrich (\_) und Doppelpunkt (:).

5. Wählen Sie **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen** aus, um anderen Mitgliedern der Rolle das Anzeigen von Ressourcen wie Volumes und Hosts zu ermöglichen, nachdem sie die Ressourcenliste aktualisiert haben.

Sie sollten diese Option deaktivieren, wenn Sie nicht möchten, dass Mitglieder dieser Rolle Objekte sehen, denen andere Mitglieder zugewiesen sind.



Wenn diese Option aktiviert ist, ist es nicht erforderlich, Benutzern Zugriff auf Objekte oder Ressourcen zuzuweisen, wenn die Benutzer derselben Rolle angehören wie der Benutzer, der die Objekte oder Ressourcen erstellt hat.

6. Wählen Sie auf der Seite „Berechtigungen“ die Berechtigungen aus, die Sie der Rolle zuweisen möchten, oder klicken Sie auf **Alle auswählen**, um der Rolle alle Berechtigungen zu erteilen.
7. Klicken Sie auf **Senden**.

## Hinzufügen einer NetApp ONTAP RBAC-Rolle mithilfe von Sicherheitsanmeldebefehlen

Sie können die Sicherheitsanmeldebefehle verwenden, um eine NetApp ONTAP RBAC-Rolle hinzuzufügen, wenn auf Ihren Speichersystemen Clustered ONTAP ausgeführt wird.

### Bevor Sie beginnen

- Identifizieren Sie die Aufgabe (oder Aufgaben), die Sie ausführen möchten, und die Berechtigungen, die zum Ausführen dieser Aufgaben erforderlich sind.
- Erteilen Sie Berechtigungen für Befehle und/oder Befehlsverzeichnisse.

Für jeden Befehl/jedes Befehlsverzeichnis gibt es zwei Zugriffsebenen: Vollzugriff und schreibgeschützt.

Sie müssen immer zuerst die Vollzugriffsrechte zuweisen.

- Weisen Sie Benutzern Rollen zu.
- Identifizieren Sie Ihre Konfiguration, je nachdem, ob Ihre SnapCenter Plug-Ins mit der Cluster-Administrator-IP für den gesamten Cluster oder direkt mit einer SVM innerhalb des Clusters verbunden sind.

## Informationen zu diesem Vorgang

Um die Konfiguration dieser Rollen auf Speichersystemen zu vereinfachen, können Sie das Tool „RBAC User Creator für NetApp ONTAP“ verwenden, das im NetApp Communities Forum veröffentlicht wird.

Dieses Tool kümmert sich automatisch um die korrekte Einrichtung der ONTAP Berechtigungen. Beispielsweise fügt das Tool RBAC User Creator für NetApp ONTAP die Berechtigungen automatisch in der richtigen Reihenfolge hinzu, sodass die Berechtigungen für den uneingeschränkten Zugriff zuerst angezeigt werden. Wenn Sie zuerst die Nur-Lese-Berechtigungen und dann die Vollzugriffsberechtigungen hinzufügen, markiert ONTAP die Vollzugriffsberechtigungen als Duplikate und ignoriert sie.



Wenn Sie SnapCenter oder ONTAP später aktualisieren, sollten Sie das Tool RBAC User Creator für NetApp ONTAP erneut ausführen, um die zuvor erstellten Benutzerrollen zu aktualisieren. Für eine frühere Version von SnapCenter oder ONTAP erstellte Benutzerrollen funktionieren mit aktualisierten Versionen nicht ordnungsgemäß. Wenn Sie das Tool erneut ausführen, wird das Upgrade automatisch durchgeführt. Sie müssen die Rollen nicht neu erstellen.

Weitere Informationen zum Einrichten von ONTAP RBAC-Rollen finden Sie im ["ONTAP 9 Administrator-Authentifizierung und RBAC Power Guide"](#).

## Schritte

1. Erstellen Sie auf dem Speichersystem eine neue Rolle, indem Sie den folgenden Befehl eingeben:

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

- svm\_name ist der Name der SVM. Wenn Sie dieses Feld leer lassen, wird standardmäßig der Clusteradministrator verwendet.
- role\_name ist der Name, den Sie für die Rolle angeben.
- Befehl ist die ONTAP Fähigkeit.



Sie müssen diesen Befehl für jede Berechtigung wiederholen. Denken Sie daran, dass Befehle mit vollem Zugriff vor schreibgeschützten Befehlen aufgeführt werden müssen.

Informationen zur Liste der Berechtigungen finden Sie unter ["ONTAP CLI-Befehle zum Erstellen von Rollen und Zuweisen von Berechtigungen"](#).

2. Erstellen Sie einen Benutzernamen, indem Sie den folgenden Befehl eingeben:

```
security login create -username <user_name\> -application ontapi -authmethod  
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment  
"user_description"
```

- Benutzername ist der Name des Benutzers, den Sie erstellen.
- <Passwort> ist Ihr Passwort. Wenn Sie kein Kennwort angeben, werden Sie vom System zur Eingabe eines Kennworts aufgefordert.
- svm\_name ist der Name der SVM.

3. Weisen Sie dem Benutzer die Rolle zu, indem Sie den folgenden Befehl eingeben:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod <password\>
```

- <Benutzername> ist der Name des Benutzers, den Sie in Schritt 2 erstellt haben. Mit diesem Befehl können Sie den Benutzer ändern, um ihn der Rolle zuzuordnen.
- <svm\_name> ist der Name der SVM.
- <role\_name> ist der Name der Rolle, die Sie in Schritt 1 erstellt haben.
- <Passwort> ist Ihr Passwort. Wenn Sie kein Kennwort angeben, werden Sie vom System zur Eingabe eines Kennworts aufgefordert.

4. Überprüfen Sie, ob der Benutzer korrekt erstellt wurde, indem Sie den folgenden Befehl eingeben:

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user\_name ist der Name des Benutzers, den Sie in Schritt 3 erstellt haben.

## Erstellen Sie SVM-Rollen mit minimalen Berechtigungen

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen müssen, wenn Sie eine Rolle für einen neuen SVM-Benutzer in ONTAP erstellen. Diese Rolle ist erforderlich, wenn Sie SVMs in ONTAP für die Verwendung mit SnapCenter konfigurieren und die Rolle „vsadmin“ nicht verwenden möchten.

### Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <svm_name\> -role <SVM_Role_Name\>  
-cmddirname <permission\>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer und weisen Sie diesem Benutzer die Rolle zu.

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

## ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "job history show" -access all

- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "job show" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "lun" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname

```

"lun serial" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "network interface" -access readonly

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy add-rule" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy modify-rule" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy remove-rule" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror restore" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "snapmirror show-history" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror update" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror update-ls-set" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "version" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split start" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file show-disk-usage" -access all

```

- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname

```

"vserver cifs share delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs share show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy rule create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy rule show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "vserver iscsi connection show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver" -access readonly
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver iscsi" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume clone split status" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume managed-feature" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem map" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem create" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem delete" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem modify" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem host" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem controller" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem show" -access all

```

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`

## Erstellen Sie SVM-Rollen für ASA R2-Systeme

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen müssen, um eine Rolle für einen neuen SVM-Benutzer in ASA R2-Systemen zu erstellen. Diese Rolle ist erforderlich, wenn Sie SVMs in ASA r2-Systemen für die Verwendung mit SnapCenter konfigurieren und die Rolle „vsadmin“ nicht verwenden möchten.

### Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer und weisen Sie diesem Benutzer die Rolle zu.

```
security login create -user <user_name\> -vserver <svm_name\> -application
http -authmethod password -role <SVM_Role_Name\>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

## ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`



- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "lun" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname

"lun show" -access all

- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "version" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume modify" -access all

- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname

```

"vserver cifs share show" -access all

```

- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "nvme namespace create" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

## Erstellen Sie ONTAP Clusterrollen mit minimalen Berechtigungen

Sie sollten eine ONTAP Clusterrolle mit minimalen Berechtigungen erstellen, damit Sie die ONTAP Administratorrolle nicht verwenden müssen, um Vorgänge in SnapCenter auszuführen. Sie können mehrere ONTAP -CLI-Befehle ausführen, um die ONTAP Clusterrolle zu erstellen und Mindestberechtigungen zuzuweisen.

### Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <cluster_name>- role <role_name>-
-cmddirname <permission>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer und weisen Sie diesem Benutzer die Rolle zu.

```
security login create -user <user_name> -vserver <cluster_name> -application
ontapi http -authmethod password -role <role_name>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name> -vserver <cluster_name>
```

## ONTAP CLI-Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen sollten, um Clusterrollen zu erstellen und

## Berechtigungen zuzuweisen.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"nvme subsystem host" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem controller" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "security login" -access readonly
• security login role create -role Role_Name -cmddirname "snapmirror create"
  -vserver Cluster_name -access all
• security login role create -role Role_Name -cmddirname "snapmirror list-
  destinations" -vserver Cluster_name -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy add-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy remove-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror show-history" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror update" -access all

```



- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "version" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"volume offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot promote" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore-file" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show-delta" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume unmount" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs delete" -access all

```

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver show" -access all

### **Erstellen Sie ONTAP Clusterrollen für ASA R2-Systeme**

Sie sollten eine ONTAP Clusterrolle mit minimalen Berechtigungen erstellen, damit Sie die ONTAP Administratorrolle nicht verwenden müssen, um Vorgänge in SnapCenter auszuführen. Sie können mehrere ONTAP -CLI-Befehle ausführen, um die ONTAP

## Clusterrolle zu erstellen und Mindestberechtigungen zuzuweisen.

### Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <cluster_name\>- role <role_name\>  
-cmddirname <permission\>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer und weisen Sie diesem Benutzer die Rolle zu.

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
http -authmethod password -role <role_name\>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

### ONTAP CLI-Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen sollten, um Clusterrollen zu erstellen und Berechtigungen zuzuweisen.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

"lun show" -access all

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "security login" -access readonly
- security login role create -role Role\_Name -cmddirname "snapmirror create" -vserver Cluster\_name -access all
- security login role create -role Role\_Name -cmddirname "snapmirror list-destinations" -vserver Cluster\_name -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy create" -access all

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "version" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"volume clone show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split start" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot promote" -access all

```



- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```
"vserver export-policy rule delete" -access all
```

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume delete" show" -access all

## Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu

Um die rollenbasierte Zugriffskontrolle für SnapCenter -Benutzer zu konfigurieren, können Sie Benutzer oder Gruppen hinzufügen und Rollen zuweisen. Die Rolle bestimmt die Optionen, auf die SnapCenter -Benutzer zugreifen können.

### Bevor Sie beginnen

- Sie müssen sich mit der Rolle „SnapCenterAdmin“ angemeldet haben.
- Sie müssen die Benutzer- oder Gruppenkonten im Active Directory im Betriebssystem oder in der Datenbank erstellt haben. Sie können SnapCenter nicht zum Erstellen dieser Konten verwenden.



In Benutzernamen und Gruppennamen dürfen nur die folgenden Sonderzeichen enthalten sein: Leerzeichen ( ), Bindestrich (-), Unterstrich (\_) und Doppelpunkt (:).

- SnapCenter umfasst mehrere vordefinierte Rollen.

Sie können dem Benutzer entweder diese Rollen zuweisen oder neue Rollen erstellen.

- AD-Benutzer und AD-Gruppen, die zu SnapCenter RBAC hinzugefügt werden, müssen über die Leseberechtigung für den Benutzercontainer und den Computercontainer im Active Directory verfügen.
- Nachdem Sie einem Benutzer oder einer Gruppe eine Rolle mit den entsprechenden Berechtigungen zugewiesen haben, müssen Sie dem Benutzer Zugriff auf SnapCenter -Assets wie Hosts und Speicherverbindungen zuweisen.

Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

- Sie sollten dem Benutzer oder der Gruppe irgendwann eine Rolle zuweisen, um die Vorteile der RBAC-Berechtigungen und -Effizienz zu nutzen.
- Sie können dem Benutzer beim Erstellen des Benutzers oder der Gruppe Assets wie Host, Ressourcengruppen, Richtlinien, Speicherverbindungen, Plug-Ins und Anmeldeinformationen zuweisen.
- Die Mindestressourcen, die Sie einem Benutzer zum Ausführen bestimmter Vorgänge zuweisen sollten, sind wie folgt:

| Betrieb                          | Vermögenszuordnung                 |
|----------------------------------|------------------------------------|
| Ressourcen schützen              | Gastgeber, Politik                 |
| Sicherung                        | Host, Ressourcengruppe, Richtlinie |
| Wiederherstellen                 | Host, Ressourcengruppe             |
| Klonen                           | Host, Ressourcengruppe, Richtlinie |
| Lebenszyklus des Klon            | Gastgeber                          |
| Erstellen einer Ressourcengruppe | Gastgeber                          |

- Wenn einem Windows-Cluster oder einem DAG-Asset (Exchange Server Database Availability Group) ein neuer Knoten hinzugefügt wird und dieser neue Knoten einem Benutzer zugewiesen wird, müssen Sie das Asset dem Benutzer oder der Gruppe neu zuweisen, um den neuen Knoten in den Benutzer oder die Gruppe aufzunehmen.

Sie sollten den RBAC-Benutzer oder die RBAC-Gruppe dem Cluster oder DAG neu zuweisen, um den neuen Knoten in den RBAC-Benutzer oder die RBAC-Gruppe aufzunehmen. Sie verfügen beispielsweise über einen Cluster mit zwei Knoten und haben dem Cluster einen RBAC-Benutzer oder eine RBAC-Gruppe zugewiesen. Wenn Sie dem Cluster einen weiteren Knoten hinzufügen, sollten Sie den RBAC-Benutzer oder die RBAC-Gruppe dem Cluster neu zuweisen, um den neuen Knoten für den RBAC-Benutzer oder die RBAC-Gruppe einzuschließen.

- Wenn Sie Snapshots replizieren möchten, müssen Sie die Speicherverbindung sowohl für das Quell- als auch für das Zielvolumen dem Benutzer zuweisen, der den Vorgang durchführt.

Sie sollten Assets hinzufügen, bevor Sie den Benutzern Zugriff zuweisen.



Wenn Sie die Funktionen des SnapCenter Plug-in for VMware vSphere zum Schutz von VMs, VMDKs oder Datenspeichern verwenden, sollten Sie die VMware vSphere-GUI verwenden, um einen vCenter-Benutzer zu einer SnapCenter Plug-in for VMware vSphere hinzuzufügen. Informationen zu VMware vSphere-Rollen finden Sie unter ["Vordefinierte Rollen im SnapCenter Plug-in for VMware vSphere"](#).

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.

2. Klicken Sie auf der Seite „Einstellungen“ auf **Benutzer und Zugriff** > \*  \*.
3. Auf der Seite „Benutzer/Gruppen aus Active Directory oder Arbeitsgruppe hinzufügen“:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zugriffstyp        | <p>Wählen Sie entweder Domäne oder Arbeitsgruppe aus</p> <p>Beim Domänenauthentifizierungstyp sollten Sie den Domännennamen des Benutzers oder der Gruppe angeben, der Sie den Benutzer zu einer Rolle hinzufügen möchten.</p> <p>Standardmäßig ist es bereits mit dem angemeldeten Domännennamen ausgefüllt.</p> <div>  <p>Sie müssen die nicht vertrauenswürdige Domäne auf der Seite <b>Einstellungen &gt; Globale Einstellungen &gt; Domäneneinstellungen</b> registrieren.</p> </div> |
| Typ                | <p>Wählen Sie entweder „Benutzer“ oder „Gruppe“ aus.</p> <div>  <p>SnapCenter unterstützt nur Sicherheitsgruppen und nicht die Verteilergruppe.</p> </div>                                                                                                                                                                                                                                                                                                                               |

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername       | <p>a. Geben Sie den Teil des Benutzernamens ein und klicken Sie dann auf <b>Hinzufügen</b>.</p> <div>  <p>Beim Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden.</p> </div> <p>b. Wählen Sie den Benutzernamen aus der Suchliste aus.</p> <div>  <p>Wenn Sie Benutzer aus einer anderen oder nicht vertrauenswürdigen Domäne hinzufügen, sollten Sie den Benutzernamen vollständig eingeben, da keine Suchliste für domänenübergreifende Benutzer vorhanden ist.</p> </div> <p>Wiederholen Sie diesen Schritt, um der ausgewählten Rolle weitere Benutzer oder Gruppen hinzuzufügen.</p> |
| Rollen             | Wählen Sie die Rolle aus, zu der Sie den Benutzer hinzufügen möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

4. Klicken Sie auf **Zuweisen** und dann auf der Seite „Assets zuweisen“:

- Wählen Sie den Asset-Typ aus der Dropdown-Liste **Asset** aus.
- Wählen Sie in der Asset-Tabelle das Asset aus.

Die Assets werden nur aufgelistet, wenn der Benutzer die Assets zu SnapCenter hinzugefügt hat.

- Wiederholen Sie diesen Vorgang für alle erforderlichen Assets.
- Klicken Sie auf **Speichern**.

5. Klicken Sie auf **Senden**.

Aktualisieren Sie die Ressourcenliste, nachdem Sie Benutzer oder Gruppen hinzugefügt und Rollen zugewiesen haben.

## Konfigurieren der Überwachungsprotokolleinstellungen

Für jede einzelne Aktivität des SnapCenter -Servers werden Prüfprotokolle generiert. Standardmäßig werden Überwachungsprotokolle am standardmäßigen Installationsort *C:\Programme\ NetApp\ SnapCenter WebApp\audit\* gesichert.

Prüfprotokolle werden durch die Generierung digital signierter Zusammenfassungen für jedes einzelne Prüfereignis gesichert, um sie vor unbefugten Änderungen zu schützen. Die generierten Digests werden in

einer separaten Prüfsummendatei gespeichert und regelmäßigen Integritätsprüfungen unterzogen, um die Integrität des Inhalts sicherzustellen.

Sie sollten sich mit der Rolle „SnapCenterAdmin“ angemeldet haben.

### Informationen zu diesem Vorgang

- In den folgenden Szenarien werden Warnungen gesendet:
  - Zeitplan für die Integritätsprüfung des Audit-Protokolls oder Syslog-Server ist aktiviert oder deaktiviert
  - Integritätsprüfung des Überwachungsprotokolls, Überwachungsprotokoll oder Syslog-Serverprotokollfehler
  - Wenig Speicherplatz
- Eine E-Mail wird nur gesendet, wenn die Integritätsprüfung fehlschlägt.
- Sie sollten die Verzeichnispfade für das Überwachungsprotokoll und das Überwachungsprüfsummenprotokoll gemeinsam ändern. Sie können nicht nur einen davon ändern.
- Wenn die Verzeichnispfade für das Prüfprotokoll und das Prüfsummenprotokoll geändert werden, kann die Integritätsprüfung für die am früheren Speicherort vorhandenen Prüfprotokolle nicht durchgeführt werden.
- Die Verzeichnispfade für das Überwachungsprotokoll und das Überwachungsprüfsummenprotokoll sollten sich auf dem lokalen Laufwerk des SnapCenter -Servers befinden.

Gemeinsam genutzte oder im Netzwerk bereitgestellte Laufwerke werden nicht unterstützt.

- Wenn in den Syslog-Servereinstellungen das UDP-Protokoll verwendet wird, können Fehler aufgrund eines ausgefallenen oder nicht verfügbaren Ports in SnapCenter weder als Fehler noch als Warnung erfasst werden.
- Sie können die Überwachungsprotokolle mit den Befehlen „Set-SmAuditSettings“ und „Get-SmAuditSettings“ konfigurieren.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von Get-Help command\_name. Alternativ können Sie auch die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

### Schritte

1. Navigieren Sie auf der Seite **Einstellungen** zu **Einstellungen > Globale Einstellungen > Einstellungen für Überwachungsprotokoll**.
2. Geben Sie im Abschnitt „Überwachungsprotokoll“ die Details ein.
3. Geben Sie das **Audit-Protokollverzeichnis** und das **Audit-Prüfsummenprotokollverzeichnis** ein
  - a. Geben Sie die maximale Dateigröße ein
  - b. Geben Sie die maximale Anzahl an Protokolldateien ein
  - c. Geben Sie den Prozentsatz der Speicherplatznutzung ein, um eine Warnung zu senden
4. (Optional) Aktivieren Sie **UTC-Zeit protokollieren**.
5. (Optional) Aktivieren Sie **Zeitplan für Integritätsprüfung des Audit-Protokolls** und klicken Sie auf **Integritätsprüfung starten**, um die Integritätsprüfung bei Bedarf durchzuführen.

Sie können auch den Befehl **Start-SmAuditIntegrityCheck** ausführen, um die Integritätsprüfung bei Bedarf zu starten.

6. (Optional) Aktivieren Sie „Überwachungsprotokolle an Remote-Syslog-Server weiterleiten“ und geben Sie

die Syslog-Serverdetails ein.

Sie sollten das Zertifikat vom Syslog-Server in das „Trusted Root“ für das TLS 1.2-Protokoll importieren.

- a. Geben Sie den Syslog-Server-Host ein
- b. Geben Sie den Syslog-Server-Port ein
- c. Geben Sie das Syslog-Serverprotokoll ein
- d. RFC-Format eingeben

7. Klicken Sie auf **Speichern**.

8. Sie können Audit-Integritätsprüfungen und Festplattenspeicherprüfungen anzeigen, indem Sie auf **Überwachen > Jobs** klicken.

## Konfigurieren Sie sichere MySQL-Verbindungen mit SnapCenter Server

Sie können Secure Sockets Layer (SSL)-Zertifikate und Schlüsseldateien generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL Server in eigenständigen Konfigurationen oder Network Load Balancing (NLB)-Konfigurationen sichern möchten.

### Konfigurieren Sie gesicherte MySQL-Verbindungen für eigenständige SnapCenter -Serverkonfigurationen

Sie können Secure Sockets Layer (SSL)-Zertifikate und Schlüsseldateien generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL Server sichern möchten. Sie müssen die Zertifikate und Schlüsseldateien im MySQL-Server und SnapCenter -Server konfigurieren.

Folgende Zertifikate werden generiert:

- CA-Zertifikat
- Öffentliches Serverzertifikat und private Schlüsseldatei
- Öffentliches Client-Zertifikat und private Schlüsseldatei

### Schritte

1. Richten Sie die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mit dem Befehl openssl ein.

Weitere Informationen finden Sie unter ["MySQL Version 5.7: Erstellen von SSL-Zertifikaten und Schlüsseln mit openssl"](#)



Der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendete allgemeine Namenswert muss sich jeweils vom allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen die Zertifikats- und Schlüsseldateien für Server fehl, die mit OpenSSL kompiliert wurden.

**Best Practice:** Sie sollten den vollqualifizierten Domännennamen (FQDN) des Servers als allgemeinen Namen für das Serverzertifikat verwenden.

2. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den MySQL-Datenordner.

Der Standardpfad des MySQL-Datenordners lautet C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Aktualisieren Sie die Pfade des CA-Zertifikats, des öffentlichen Serverzertifikats, des öffentlichen Clientzertifikats, des privaten Serverschlüssels und des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

Der Standardpfad der MySQL-Serverkonfigurationsdatei (my.ini) lautet C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini.



Sie müssen das CA-Zertifikat, das öffentliche Serverzertifikat und die privaten Schlüsselpfade des Servers im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Sie müssen das CA-Zertifikat, das öffentliche Client-Zertifikat und die privaten Schlüsselpfade des Clients im Abschnitt [client] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Das folgende Beispiel zeigt die Zertifikate und Schlüsseldateien, die in den Abschnitt [mysqld] der Datei my.ini im Standardordner kopiert wurden. C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

Das folgende Beispiel zeigt die im Abschnitt [client] der Datei my.ini aktualisierten Pfade.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. Stoppen Sie die SnapCenter Server-Webanwendung im Internet Information Server (IIS).



5. Starten Sie den MySQL-Dienst neu.
6. Aktualisieren Sie den Wert des MySQLProtocol-Schlüssels in der SnapManager Datei .Web.UI.dll.config.

Das folgende Beispiel zeigt den Wert des MySQLProtocol-Schlüssels, der in der SnapManager Datei .Web.UI.dll.config aktualisiert wurde.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Aktualisieren Sie die Datei SnapManager.Web.UI.dll.config mit den Pfaden, die im Abschnitt [client] der Datei my.ini angegeben wurden.

Das folgende Beispiel zeigt die im Abschnitt [client] der Datei my.ini aktualisierten Pfade.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/ca.pem" />
```

8. Starten Sie die SnapCenter Server-Webanwendung im IIS.

## Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen

Sie können Secure Sockets Layer (SSL)-Zertifikate und Schlüsseldateien für beide High Availability (HA)-Knoten generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL-Servern sichern möchten. Sie müssen die Zertifikate und Schlüsseldateien auf den MySQL-Servern und auf den HA-Knoten konfigurieren.

Folgende Zertifikate werden generiert:

- CA-Zertifikat

Auf einem der HA-Knoten wird ein CA-Zertifikat generiert und dieses CA-Zertifikat wird auf den anderen HA-Knoten kopiert.

- Öffentliches Serverzertifikat und private Serverschlüsseldateien für beide HA-Knoten
- Öffentliches Client-Zertifikat und private Client-Schlüsseldateien für beide HA-Knoten

## Schritte

1. Richten Sie für den ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mit dem Befehl openssl ein.

Weitere Informationen finden Sie unter ["MySQL Version 5.7: Erstellen von SSL-Zertifikaten und Schlüsseln mit openssl"](#)



Der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendete allgemeine Namenswert muss sich jeweils vom allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen die Zertifikats- und Schlüsseldateien für Server fehl, die mit OpenSSL kompiliert wurden.

**Best Practice:** Sie sollten den vollqualifizierten Domännennamen (FQDN) des Servers als allgemeinen Namen für das Serverzertifikat verwenden.

2. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den MySQL-Datenordner.

Der Standardpfad des MySQL-Datenordners lautet C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

3. Aktualisieren Sie die Pfade des CA-Zertifikats, des öffentlichen Serverzertifikats, des öffentlichen Clientzertifikats, des privaten Serverschlüssels und des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

Der Standardpfad der MySQL-Serverkonfigurationsdatei (my.ini) lautet C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini.



Sie müssen die Pfade für das CA-Zertifikat, das öffentliche Serverzertifikat und den privaten Schlüssel des Servers im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Sie müssen die Pfade des CA-Zertifikats, des öffentlichen Client-Zertifikats und des privaten Client-Schlüssels im Abschnitt [client] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Das folgende Beispiel zeigt die Zertifikate und Schlüsseldateien, die in den Abschnitt [mysqld] der Datei my.ini im Standardordner C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data kopiert wurden.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

Das folgende Beispiel zeigt die im Abschnitt [client] der Datei my.ini aktualisierten Pfade.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. Kopieren Sie für den zweiten HA-Knoten das CA-Zertifikat und generieren Sie ein öffentliches Serverzertifikat, private Serverschlüsseldateien, ein öffentliches Clientzertifikat und private Clientschlüsseldateien. Führen Sie die folgenden Schritte aus:
  - a. Kopieren Sie das auf dem ersten HA-Knoten generierte CA-Zertifikat in den MySQL-Datenordner des zweiten NLB-Knotens.

Der Standardpfad des MySQL-Datenordners lautet C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.



Sie müssen kein CA-Zertifikat erneut erstellen. Sie sollten nur das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, die private Schlüsseldatei des Servers und die private Schlüsseldatei des Clients erstellen.

- b. Richten Sie für den ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mit dem Befehl openssl ein.

#### "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und Schlüsseln mit openssl"



Der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendete allgemeine Namenswert muss sich jeweils vom allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen die Zertifikats- und Schlüsseldateien für Server fehl, die mit OpenSSL kompiliert wurden.

Es wird empfohlen, den Server-FQDN als allgemeinen Namen für das Serverzertifikat zu verwenden.

- c. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den MySQL-Datenordner.
  - d. Aktualisieren Sie die Pfade des CA-Zertifikats, des öffentlichen Serverzertifikats, des öffentlichen Clientzertifikats, des privaten Serverschlüssels und des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).



Sie müssen das CA-Zertifikat, das öffentliche Serverzertifikat und die privaten Schlüsselpfade des Servers im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Sie müssen das CA-Zertifikat, das öffentliche Client-Zertifikat und die privaten Schlüsselpfade des Clients im Abschnitt [client] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

Das folgende Beispiel zeigt die Zertifikate und Schlüsseldateien, die in den Abschnitt [mysqld] der Datei my.ini im Standardordner C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data kopiert wurden.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

Das folgende Beispiel zeigt die im Abschnitt [client] der Datei my.ini aktualisierten Pfade.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

5. Stoppen Sie die SnapCenter Server-Webanwendung im Internet Information Server (IIS) auf beiden HA-Knoten.
6. Starten Sie den MySQL-Dienst auf beiden HA-Knoten neu.
7. Aktualisieren Sie den Wert des MySQLProtocol-Schlüssels in der SnapManager Datei .Web.UI.dll.config für beide HA-Knoten.

Das folgende Beispiel zeigt den Wert des MySQLProtocol-Schlüssels, der in der Datei SnapManager.Web.UI.dll.config aktualisiert wurde.

```
<add key="MySQLProtocol" value="SSL" />
```

8. Aktualisieren Sie die Datei SnapManager.Web.UI.dll.config mit den Pfaden, die Sie im Abschnitt [client] der Datei my.ini für beide HA-Knoten angegeben haben.

Das folgende Beispiel zeigt die im Abschnitt [client] der my.ini-Dateien aktualisierten Pfade.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. Starten Sie die SnapCenter Server-Webanwendung im IIS auf beiden HA-Knoten.
10. Verwenden Sie das PowerShell-Cmdlet „Set-SmRepositoryConfig -RebuildSlave -Force“ mit der Option „-Force“ auf einem der HA-Knoten, um eine sichere MySQL-Replikation auf beiden HA-Knoten einzurichten.

Auch wenn der Replikationsstatus fehlerfrei ist, können Sie mit der Option -Force das Slave-Repository neu erstellen.

## Konfigurieren der zertifikatsbasierten Authentifizierung

Die zertifikatsbasierte Authentifizierung erhöht die Sicherheit, indem sie die Identität sowohl des SnapCenter Servers als auch der Plug-in-Hosts überprüft und so eine sichere und verschlüsselte Kommunikation gewährleistet.

### Zertifikatsbasierte Authentifizierung aktivieren

Um die zertifikatsbasierte Authentifizierung für SnapCenter Server und die Windows-Plug-In-Hosts zu aktivieren, führen Sie das folgende PowerShell-Cmdlet aus. Für die Linux-Plug-in-Hosts wird die zertifikatsbasierte Authentifizierung aktiviert, wenn Sie das bidirektionale SSL aktivieren.

- So aktivieren Sie die Client-Zertifikat-basierte Authentifizierung:

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- So deaktivieren Sie die Client-Zertifikat-basierte Authentifizierung:

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

### Exportieren Sie Zertifikate der Zertifizierungsstelle (CA) vom SnapCenter Server

Sie sollten die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) vom SnapCenter -Server auf die Plug-In-Hosts exportieren.

#### Bevor Sie beginnen

Sie sollten das bidirektionale SSL konfiguriert haben.

## Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster „Zertifikat-Snap-In“ die Option **Computerkonto** und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Persönlich > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf das beschaffte CA-Zertifikat, das für SnapCenter Server verwendet wird, und wählen Sie dann **Alle Aufgaben > Exportieren**, um den Exportassistenten zu starten.
6. Führen Sie im Assistenten die folgenden Aktionen aus.

| Für diese Option...                          | Gehen Sie wie folgt vor...                                                                                                        |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel exportieren               | Wählen Sie <b>Nein, privaten Schlüssel nicht exportieren</b> und klicken Sie dann auf <b>Weiter</b> .                             |
| Exportdateiformat                            | Klicken Sie auf <b>Weiter</b> .                                                                                                   |
| Dateiname                                    | Klicken Sie auf <b>Durchsuchen</b> , geben Sie den Dateipfad zum Speichern des Zertifikats an und klicken Sie auf <b>Weiter</b> . |
| Abschließen des Zertifikatexport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Export zu starten.                             |



Die zertifikatsbasierte Authentifizierung wird für SnapCenter HA-Konfigurationen und das SnapCenter Plug-in for VMware vSphere nicht unterstützt.

## Importieren Sie das CA-Zertifikat in die Windows-Plug-In-Hosts

Um das exportierte SnapCenter Server CA-Zertifikat zu verwenden, sollten Sie das zugehörige Zertifikat mithilfe der Microsoft Management Console (MMC) in die SnapCenter Windows-Plug-In-Hosts importieren.

## Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster „Zertifikat-Snap-In“ die Option **Computerkonto** und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Persönlich > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Persönlich“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Führen Sie im Assistenten die folgenden Aktionen aus.

| Für diese Option...                          | Gehen Sie wie folgt vor...                                                                            |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Standort des Geschäfts                       | Klicken Sie auf <b>Weiter</b> .                                                                       |
| Zu importierende Datei                       | Wählen Sie das SnapCenter Server-Zertifikat mit der Erweiterung .cer aus.                             |
| Zertifikatspeicher                           | Klicken Sie auf <b>Weiter</b> .                                                                       |
| Abschließen des Zertifikatexport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten. |

## Importieren Sie das CA-Zertifikat in die UNIX-Plug-in-Hosts

Sie sollten das CA-Zertifikat in die UNIX-Plug-in-Hosts importieren.

### Über diese Aufgabe

- Sie können das Kennwort für den SPL-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars verwalten.
- Das Kennwort für den SPL-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels sollten identisch sein.

### Schritte

1. Sie können das Standardkennwort für den SPL-Schlüsselspeicher aus der SPL-Eigenschaftendatei abrufen. Es ist der Wert, der dem Schlüssel entspricht `SPL_KEYSTORE_PASS`.
2. Ändern Sie das Keystore-Passwort:  

```
$ keytool -storepasswd -keystore keystore.jks
```
3. 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
```
4. Aktualisieren Sie dasselbe für den Schlüssel `SPL_KEYSTORE_PASS` in `spl.properties` Datei.
5. Starten Sie den Dienst nach der Änderung des Kennworts neu.

## Konfigurieren Sie Stamm- oder Zwischenzertifikate für den SPL-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate für den SPL-Truststore konfigurieren. Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

### Schritte

1. Navigieren Sie zu dem 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
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported>
-file /<CertificatePath> -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den SPL-Truststore konfiguriert haben.

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

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

### Schritte

1. Navigieren Sie zu dem Ordner, der den Schlüsselspeicher der SPL 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
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype
pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
$ keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.

7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

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

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

8. Wenn der Aliasname im CA-Zertifikat lang ist und Leerzeichen oder Sonderzeichen („\*“, „“, „“) enthält, ändern Sie den Aliasnamen in einen einfachen Namen:

```
$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>"
-keystore keystore.jks`
```

9. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher in `spl.properties` Datei. Aktualisieren Sie diesen Wert anhand des Schlüssels `SPL_CERTIFICATE_ALIAS`.

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

## Exportieren von SnapCenter -Zertifikaten

Sie sollten die SnapCenter -Zertifikate im .pfx-Format exportieren.

### Schritte



1. Gehen Sie zur Microsoft-Verwaltungskontrolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Mein Benutzerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Aktueller Benutzer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf das Zertifikat mit dem SnapCenter -Anzeigenamen und wählen Sie dann **Alle Aufgaben > Exportieren**, um den Exportassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel exportieren               | Wählen Sie die Option <b>Ja, privaten Schlüssel exportieren</b> und klicken Sie anschließend auf <b>Weiter</b> .                   |
| Exportdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Zu exportierende Datei                       | Geben Sie einen Dateinamen für das exportierte Zertifikat an (Sie müssen .pfx verwenden) und klicken Sie dann auf <b>Weiter</b> .  |
| Abschließen des Zertifikatexport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Export zu starten.                              |

## Konfigurieren des CA-Zertifikats für den Windows-Host

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

## CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

## Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
  - a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-ChildItem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

## Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## Konfigurieren des CA-Zertifikats mit der SnapCenter -Site

Sie sollten das CA-Zertifikat mit der SnapCenter -Site auf dem Windows-Host konfigurieren.

### Schritte

1. Öffnen Sie den IIS-Manager auf dem Windows-Server, auf dem SnapCenter installiert ist.
2. Klicken Sie im linken Navigationsbereich auf **Verbindungen**.
3. Erweitern Sie den Namen des Servers und **Sites**.
4. Wählen Sie die SnapCenter -Website aus, auf der Sie das SSL-Zertifikat installieren möchten.
5. Navigieren Sie zu **Aktionen > Site bearbeiten** und klicken Sie auf **Bindungen**.
6. Wählen Sie auf der Seite „Bindungen“ die Option **Bindung für https** aus.
7. Klicken Sie auf **Bearbeiten**.
8. Wählen Sie aus der Dropdown-Liste „SSL-Zertifikat“ das kürzlich importierte SSL-Zertifikat aus.
9. Klicken Sie auf **OK**.



Die SnapCenter Scheduler-Site (Standardport: 8154, HTTPS) ist mit einem selbstsignierten Zertifikat konfiguriert. Dieser Port kommuniziert innerhalb des SnapCenter Server-Hosts und muss nicht mit einem CA-Zertifikat konfiguriert werden. Wenn Ihre Umgebung jedoch die Verwendung eines CA-Zertifikats erfordert, wiederholen Sie die Schritte 5 bis 9 mithilfe der SnapCenter Scheduler-Site.



Wenn das kürzlich bereitgestellte CA-Zertifikat nicht im Dropdown-Menü aufgeführt ist, überprüfen Sie, ob das CA-Zertifikat mit dem privaten Schlüssel verknüpft ist.



Stellen Sie sicher, dass das Zertifikat über den folgenden Pfad hinzugefügt wird:  
**Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate.**

## Aktivieren von CA-Zertifikaten für SnapCenter

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikatvalidierung für den SnapCenter -Server aktivieren.

### Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „Set-SmCertificateSettings“ aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für den SnapCenter -Server mit dem Cmdlet Get-SmCertificateSettings anzeigen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command\_name*. Alternativ können Sie sich an die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

### Schritte

1. Navigieren Sie auf der Seite „Einstellungen“ zu **Einstellungen > Globale Einstellungen > CA-Zertifikateinstellungen**.
2. Wählen Sie **Zertifikatvalidierung aktivieren**.
3. Klicken Sie auf **Übernehmen**.

### Nachdem Sie fertig sind

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 für den Plug-In-Host kein CA-Zertifikat aktiviert oder 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.

## Konfigurieren des CA-Zertifikats für den Linux-Host

Nach der Installation des SnapCenter -Servers unter Linux erstellt das Installationsprogramm das selbstsignierte Zertifikat. Wenn Sie das CA-Zertifikat verwenden möchten, sollten Sie die Zertifikate für den Nginx-Reverse-Proxy, die Audit-Protokollierung und die SnapCenter -Dienste konfigurieren.

### Konfigurieren Sie das Nginx-Zertifikat

#### Schritte

1. Navigieren Sie zu */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Öffnen Sie **snapcenter.conf** mit vi oder einem beliebigen Texteditor.
3. Navigieren Sie zum Serverabschnitt in der Konfigurationsdatei.

4. Ändern Sie die Pfade von *ssl\_certificate* und *ssl\_certificate\_key*, sodass sie auf das CA-Zertifikat verweisen.
5. Speichern und schließen Sie die Datei.
6. Nginx neu laden: `$nginx -s reload`

## Konfigurieren des Überwachungsprotokollzertifikats

### Schritte

1. Öffnen Sie *INSTALL\_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config* mit vi oder einem beliebigen Texteditor.

Der Standardwert von *INSTALL\_DIR* ist */opt*.

2. Bearbeiten Sie die Schlüssel **AUDILOG\_CERTIFICATE\_PATH** und **AUDILOG\_CERTIFICATE\_PASSWORD**, um den CA-Zertifikatpfad bzw. das CA-Passwort einzuschließen.

Für das Audit-Protokollzertifikat wird nur das *.pfx*-Format unterstützt.

3. Speichern und schließen Sie die Datei.
4. Starten Sie den Dienst **snapmanagerweb** neu: `$ systemctl restart snapmanagerweb`

## Konfigurieren des SnapCenter -Dienstzertifikats

### Schritte

1. Öffnen Sie die folgenden Konfigurationsdateien mit vi oder einem beliebigen Texteditor.
  - *INSTALL\_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
  - *INSTALL\_DIR/ NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*
  - *INSTALL\_DIR/ NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config*

Der Standardwert von *INSTALL\_DIR* ist */opt*.

2. Bearbeiten Sie die Schlüssel **SERVICE\_CERTIFICATE\_PATH** und **SERVICE\_CERTIFICATE\_PASSWORD**, um den CA-Zertifikatpfad bzw. das CA-Passwort einzuschließen.

Für das SnapCenter -Dienstzertifikat wird nur das *.pfx*-Format unterstützt.

3. Speichern und schließen Sie die Dateien.
4. Starten Sie alle Dienste neu.
  - `$ systemctl restart snapmanagerweb`
  - `$ systemctl restart smcore`
  - `$ systemctl restart scheduler`

## Konfigurieren und Aktivieren der bidirektionalen SSL-Kommunikation auf dem Windows-Host

## Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Sie sollten die bidirektionale SSL-Kommunikation konfigurieren, um die gegenseitige Kommunikation zwischen dem SnapCenter Server auf dem Windows-Host und den Plug-Ins zu sichern.

### Bevor Sie beginnen

- Sie sollten die CSR-Datei des CA-Zertifikats mit der minimal unterstützten Schlüssellänge von 3072 generiert haben.
- Das CA-Zertifikat sollte die Server- und Client-Authentifizierung unterstützen.
- Sie sollten über ein CA-Zertifikat mit privatem Schlüssel und Fingerabdruckdetails verfügen.
- Sie sollten die Einweg-SSL-Konfiguration aktiviert haben.

Weitere Einzelheiten finden Sie unter ["Abschnitt „CA-Zertifikat konfigurieren“](#).

- Sie müssen die bidirektionale SSL-Kommunikation auf allen Plug-In-Hosts und dem SnapCenter -Server aktiviert haben.

Umgebungen mit einigen Hosts oder Servern, die nicht für die bidirektionale SSL-Kommunikation aktiviert sind, werden nicht unterstützt.

### Schritte

1. Um den Port zu binden, führen Sie mithilfe von PowerShell-Befehlen die folgenden Schritte auf dem SnapCenter Server-Host für den SnapCenter IIS-Webserver-Port 8146 (Standard) und noch einmal für den SMCORE-Port 8145 (Standard) aus.

- a. Entfernen Sie die vorhandene selbstsignierte Zertifikat-Portbindung von SnapCenter mit dem folgenden PowerShell-Befehl.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

Zum Beispiel,

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. Binden Sie das neu erworbene CA-Zertifikat an den SnapCenter -Server und den SMCORE-Port.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Zum Beispiel,

```

> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145

```

2. Um auf die Berechtigung für das CA-Zertifikat zuzugreifen, fügen Sie den standardmäßigen IIS-Webserverbenutzer „**IIS AppPool\ SnapCenter**“ des SnapCenters zur Zertifikatberechtigungsliste hinzu, indem Sie die folgenden Schritte ausführen, um auf das neu erworbene CA-Zertifikat zuzugreifen.
  - a. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > SnapIn hinzufügen/entfernen**.
  - b. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
  - c. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
  - d. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Persönlich > Zertifikate**.
  - e. Wählen Sie das SnapCenter -Zertifikat aus.
  - f. Um den Assistenten zum Hinzufügen von Benutzern/Berechtigungen zu starten, klicken Sie mit der rechten Maustaste auf das CA-Zertifikat und wählen Sie **Alle Aufgaben > Private Schlüssel verwalten**.
  - g. Klicken Sie auf **Hinzufügen** und ändern Sie im Assistenten „Benutzer und Gruppen auswählen“ den Speicherort in den lokalen Computernamen (ganz oben in der Hierarchie).
  - h. Fügen Sie den IIS AppPool\ SnapCenter Benutzer hinzu und erteilen Sie ihm die Vollzugriffsberechtigung.
3. Fügen Sie für die **IIS-Berechtigung des CA-Zertifikats** den neuen DWORD-Registrierungsschlüsseleintrag in SnapCenter Server aus dem folgenden Pfad hinzu:

Navigieren Sie im Windows-Registrierungseditor zum unten angegebenen Pfad.

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. Erstellen Sie einen neuen DWORD-Registrierungsschlüsseleintrag im Kontext der SCHANNEL-Registrierungskonfiguration.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```



## Konfigurieren Sie das SnapCenter Windows-Plug-In für die bidirektionale SSL-Kommunikation

Sie sollten das SnapCenter Windows-Plug-In für die bidirektionale SSL-Kommunikation mithilfe von PowerShell-Befehlen konfigurieren.

### Bevor Sie beginnen

Stellen Sie sicher, dass der Fingerabdruck des CA-Zertifikats verfügbar ist.

### Schritte

1. Um den Port zu binden, führen Sie die folgenden Aktionen auf dem Windows-Plug-In-Host für SMCore-Port 8145 (Standard) aus.

- a. Entfernen Sie die vorhandene selbstsignierte Zertifikat-Portbindung von SnapCenter mit dem folgenden PowerShell-Befehl.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

Zum Beispiel,

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. Binden Sie das neu erworbene CA-Zertifikat an den SMCore-Port.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

Zum Beispiel,

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

## Aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Sie können die bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige Kommunikation zwischen SnapCenter Server auf dem Windows-Host und den Plug-Ins mithilfe von PowerShell-Befehlen zu sichern.

### Bevor Sie beginnen

Führen Sie zuerst die Befehle für alle Plug-Ins und den SMCore-Agenten und dann für den Server aus.

## Schritte

1. Um die bidirektionale SSL-Kommunikation zu aktivieren, führen Sie die folgenden Befehle auf dem SnapCenter -Server für die Plug-Ins, den Server und für jeden der Agenten aus, für die die bidirektionale SSL-Kommunikation erforderlich ist.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Führen Sie den Recyclingvorgang des IIS SnapCenter -Anwendungspools mit dem folgenden Befehl durch.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Starten Sie für Windows-Plug-Ins den SMCore-Dienst neu, indem Sie den folgenden PowerShell-Befehl ausführen:

```
> Restart-Service -Name SnapManagerCoreService
```

## Deaktivieren Sie die bidirektionale SSL-Kommunikation

Sie können die bidirektionale SSL-Kommunikation mithilfe von PowerShell-Befehlen deaktivieren.

## Über diese Aufgabe

- Führen Sie zuerst die Befehle für alle Plug-Ins und den SMCore-Agenten und dann für den Server aus.
- Wenn Sie die bidirektionale SSL-Kommunikation deaktivieren, werden das CA-Zertifikat und seine Konfiguration nicht entfernt.
- Um einen neuen Host zum SnapCenter -Server hinzuzufügen, müssen Sie das bidirektionale SSL für alle Plug-In-Hosts deaktivieren.
- NLB und F5 werden nicht unterstützt.

## Schritte

1. Um die bidirektionale SSL-Kommunikation zu deaktivieren, führen Sie die folgenden Befehle auf dem SnapCenter -Server für alle Plug-In-Hosts und den SnapCenter Host aus.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Führen Sie den Recyclingvorgang des IIS SnapCenter -Anwendungspools mit dem folgenden Befehl durch.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Starten Sie für Windows-Plug-Ins den SMCore-Dienst neu, indem Sie den folgenden PowerShell-Befehl ausführen:

```
> Restart-Service -Name SnapManagerCoreService
```

## Konfigurieren und Aktivieren der bidirektionalen SSL-Kommunikation auf dem Linux-Host

### Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host

Sie sollten die bidirektionale SSL-Kommunikation konfigurieren, um die gegenseitige Kommunikation zwischen dem SnapCenter -Server auf dem Linux-Host und den Plug-Ins zu sichern.

#### Bevor Sie beginnen

- Sie sollten das CA-Zertifikat für den Linux-Host konfiguriert haben.
- Sie müssen die bidirektionale SSL-Kommunikation auf allen Plug-In-Hosts und dem SnapCenter -Server aktiviert haben.

#### Schritte

1. Kopieren Sie **certificate.pem** nach `/etc/pki/ca-trust/source/anchors/`.
2. Fügen Sie die Zertifikate zur Vertrauensliste Ihres Linux-Hosts hinzu.
  - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
  - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
  - `update-ca-trust extract`
3. Überprüfen Sie, ob die Zertifikate zur Vertrauensliste hinzugefügt wurden.  
`trust list | grep "<CN of your certificate>"`
4. Aktualisieren Sie **ssl\_certificate** und **ssl\_certificate\_key** in der SnapCenter **nginx**-Datei und starten Sie neu.
  - `vim /etc/nginx/conf.d/snapcenter.conf`
  - `systemctl restart nginx`
5. Aktualisieren Sie den SnapCenter Server-GUI-Link.
6. Aktualisieren Sie die Werte der folgenden Schlüssel in \* SnapManager\* unter `/<Installationspfad>/NetApp/snapcenter/SnapManagerWeb` und **SMCoreServiceHost.dll.config** unter `/<Installationspfad>/NetApp/snapcenter/SMCore`.
  - `<add key="SERVICE_CERTIFICATE_PATH" value="<Pfad der Datei certificate.pfx>" />`
  - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>" />`
7. Starten Sie die folgenden Dienste neu.
  - `systemctl restart smcore.service`
  - `systemctl restart snapmanagerweb.service`

8. Überprüfen Sie, ob das Zertifikat an den SnapManager -Webport angehängt ist.  
`openssl s_client -connect localhost:8146 -brief`
9. Überprüfen Sie, ob das Zertifikat an den SMCore-Port angehängt ist.  
`openssl s_client -connect localhost:8145 -brief`
10. Verwalten Sie das Kennwort für den SPL-Schlüsselspeicher und den Alias.
  - a. Rufen Sie das dem Schlüssel **SPL\_KEYSTORE\_PASS** in der SPL-Eigenschaftendatei zugewiesene Standardkennwort für den SPL-Schlüsselspeicher ab.
  - b. Ändern Sie das Keystore-Passwort.  
`keytool -storepasswd -keystore keystore.jks`
  - c. Ändern Sie das Passwort für alle Aliase der privaten Schlüsseleinträge.  
`keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  - d. Aktualisieren Sie dasselbe Passwort für den Schlüssel **SPL\_KEYSTORE\_PASS** in *spl.properties*.
  - e. Starten Sie den Dienst neu.
11. Fügen Sie auf dem Linux-Host des Plug-ins die Stamm- und Zwischenzertifikate zum Schlüsselspeicher des SPL-Plug-ins hinzu.
  - ° `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
  - ° `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
  - i. Überprüfen Sie die Einträge in keystore.jks.  
`keytool -list -v -keystore <path to keystore.jks>`
  - ii. Benennen Sie bei Bedarf alle Aliase um.  
`keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Aktualisieren Sie den Wert von **SPL\_CERTIFICATE\_ALIAS** in der Datei *spl.properties* mit dem Alias von **certificate.pfx**, der in *keystore.jks* gespeichert ist, und starten Sie den SPL-Dienst neu: `systemctl restart spl`
13. Überprüfen Sie, ob das Zertifikat an den SMCore-Port angehängt ist.  
`openssl s_client -connect localhost:8145 -brief`

## Aktivieren Sie die SSL-Kommunikation auf dem Linux-Host

Sie können die bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige Kommunikation zwischen dem SnapCenter Server auf dem Linux-Host und den Plug-Ins mithilfe von PowerShell-Befehlen zu sichern.

### Schritt

1. Führen Sie die folgenden Schritte aus, um die unidirektionale SSL-Kommunikation zu aktivieren.
  - a. Melden Sie sich bei der SnapCenter -GUI an.
  - b. Klicken Sie auf **Einstellungen > Globale Einstellungen** und wählen Sie **Zertifikatvalidierung auf SnapCenter Server aktivieren**.

c. Klicken Sie auf **Hosts > Verwaltete Hosts** und wählen Sie den Plug-in-Host aus, für den Sie unidirektionales SSL aktivieren möchten.

d. Klicken  Symbol und klicken Sie dann auf **Zertifikatvalidierung aktivieren**.

2. Aktivieren Sie die bidirektionale SSL-Kommunikation vom SnapCenter Server Linux-Host.

- `Open-SmConnection`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
- `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

## Konfigurieren von Active Directory, LDAP und LDAPS

### Registrieren nicht vertrauenswürdiger Active Directory-Domänen

Sie sollten das Active Directory beim SnapCenter Server registrieren, um Hosts, Benutzer und Gruppen aus mehreren nicht vertrauenswürdigen Active Directory-Domänen zu verwalten.

#### Bevor Sie beginnen

##### LDAP- und LDAPS-Protokolle

- Sie können die nicht vertrauenswürdigen Active Directory-Domänen entweder mit dem LDAP- oder dem LDAPS-Protokoll registrieren.
- Sie sollten die bidirektionale Kommunikation zwischen den Plug-In-Hosts und dem SnapCenter -Server aktiviert haben.
- Die DNS-Auflösung sollte vom SnapCenter -Server zu den Plug-In-Hosts und umgekehrt eingerichtet werden.

##### LDAP-Protokoll

- Der vollqualifizierte Domänenname (FQDN) sollte vom SnapCenter -Server auflösbar sein.

Sie können eine nicht vertrauenswürdige Domäne mit dem FQDN registrieren. Wenn der FQDN vom SnapCenter -Server nicht aufgelöst werden kann, können Sie sich mit einer Domänencontroller-IP-Adresse registrieren. Diese sollte vom SnapCenter -Server aufgelöst werden können.

##### LDAPS-Protokoll

- Für LDAPS sind CA-Zertifikate erforderlich, um eine End-to-End-Verschlüsselung während der Active Directory-Kommunikation bereitzustellen.

["Konfigurieren des CA-Client-Zertifikats für LDAPS"](#)

- Domänencontroller-Hostnamen (DCHostName) sollten vom SnapCenter -Server aus erreichbar sein.

#### Über diese Aufgabe

- Sie können entweder die SnapCenter -Benutzeroberfläche, PowerShell-Cmdlets oder die REST-API verwenden, um eine nicht vertrauenswürdige Domäne zu registrieren.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Klicken Sie auf der Seite „Globale Einstellungen“ auf **Domäneneinstellungen**.
4. Klicken  um eine neue Domain zu registrieren.
5. Wählen Sie auf der Seite „Neue Domäne registrieren“ entweder **LDAP** oder **LDAPS** aus.
  - a. Wenn Sie **LDAP** auswählen, geben Sie die Informationen an, die zum Registrieren der nicht vertrauenswürdigen Domäne für LDAP erforderlich sind:

| Für dieses Feld...                 | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domänenname                        | Geben Sie den NetBIOS-Namen für die Domäne an.                                                                                                                                                                                                                                                                |
| Domänen-FQDN                       | Geben Sie den FQDN an und klicken Sie auf <b>Auflösen</b> .                                                                                                                                                                                                                                                   |
| IP-Adressen des Domänencontrollers | <p>Wenn der Domänen-FQDN vom SnapCenter -Server nicht aufgelöst werden kann, geben Sie eine oder mehrere Domänencontroller-IP-Adressen an.</p> <p>Weitere Informationen finden Sie unter "<a href="#">Fügen Sie die Domänencontroller-IP für eine nicht vertrauenswürdige Domäne über die GUI hinzu</a>".</p> |

- b. Wenn Sie **LDAPS** auswählen, geben Sie die Informationen an, die zum Registrieren der nicht vertrauenswürdigen Domäne für LDAPS erforderlich sind:

| Für dieses Feld...                 | Machen Sie Folgendes...                                                                                                            |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Domänenname                        | Geben Sie den NetBIOS-Namen für die Domäne an.                                                                                     |
| Domänen-FQDN                       | Geben Sie den FQDN an.                                                                                                             |
| Domänencontrollernamen             | Geben Sie einen oder mehrere Domänencontrollernamen an und klicken Sie auf <b>Auflösen</b> .                                       |
| IP-Adressen des Domänencontrollers | Wenn die Domänencontrollernamen vom SnapCenter -Server nicht aufgelöst werden können, sollten Sie die DNS-Auflösungen korrigieren. |

6. Klicken Sie auf **OK**.

## Konfigurieren Sie IIS-Anwendungspools, um Active Directory-Leseberechtigungen zu aktivieren.

Sie können Internetinformationsdienste (IIS) auf Ihrem Windows-Server konfigurieren, um ein benutzerdefiniertes Anwendungspoolkonto zu erstellen, wenn Sie Active Directory-Leseberechtigungen für SnapCenter aktivieren müssen.

### Schritte

1. Öffnen Sie den IIS-Manager auf dem Windows-Server, auf dem SnapCenter installiert ist.
2. Klicken Sie im linken Navigationsbereich auf **Anwendungspools**.
3. Wählen Sie SnapCenter in der Liste „Anwendungspools“ aus und klicken Sie dann im Aktionsbereich auf **Erweiterte Einstellungen**.
4. Wählen Sie „Identität“ aus und klicken Sie dann auf ..., um die Identität des SnapCenter -Anwendungspools zu bearbeiten.
5. Geben Sie im Feld „Benutzerdefiniertes Konto“ den Namen eines Domänenbenutzer- oder Domänenadministratorkontos mit Active Directory-Leseberechtigung ein.
6. Klicken Sie auf OK.

Das benutzerdefinierte Konto ersetzt das integrierte ApplicationPoolIdentity-Konto für den SnapCenter -Anwendungspool.

## Konfigurieren des CA-Client-Zertifikats für LDAPS

Sie sollten das CA-Client-Zertifikat für LDAPS auf dem SnapCenter -Server konfigurieren, wenn das Windows Active Directory LDAPS mit den CA-Zertifikaten konfiguriert ist.

### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...      | Gehen Sie wie folgt vor...                                                                                         |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Auf der zweiten Seite des Assistenten | Klicken Sie auf <b>Durchsuchen</b> , wählen Sie das <i>Stammzertifikat</i> aus und klicken Sie auf <b>Weiter</b> . |

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                            |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten. |

7. Wiederholen Sie die Schritte 5 und 6 für die Zwischenzertifikate.



# Schützen Sie Microsoft SQL Server-Datenbanken

## SnapCenter -Plug-in für Microsoft SQL Server

### Übersicht über das SnapCenter -Plug-in für Microsoft SQL Server

Das SnapCenter -Plug-in für Microsoft SQL Server ist eine hostseitige Komponente der NetApp SnapCenter -Software, die eine anwendungsbewusste Datenschutzverwaltung von Microsoft SQL Server-Datenbanken ermöglicht. Das Plug-in für SQL Server automatisiert die Sicherungs-, Überprüfungs-, Wiederherstellungs- und Klonvorgänge der SQL Server-Datenbank in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für SQL Server installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und mit der NetApp SnapVault -Technologie eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards oder zu Archivierungszwecken durchführen.

- Automatisiert anwendungsbezogene Sicherungs-, Wiederherstellungs- und Klonvorgänge für Microsoft SQL Server-Datenbanken in Ihrer SnapCenter -Umgebung.
- Unterstützt Microsoft SQL Server-Datenbanken auf VMDK und Raw Device Mapping (RDM) LUNs, wenn Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren
- Unterstützt nur die Bereitstellung von SMB-Freigaben. Für die Sicherung von SQL Server-Datenbanken auf SMB-Freigaben wird keine Unterstützung bereitgestellt.
- Unterstützt das Importieren von Backups von SnapManager für Microsoft SQL Server in SnapCenter.

### Was Sie mit dem SnapCenter Plug-in für Microsoft SQL Server tun können

Wenn das SnapCenter -Plug-in für Microsoft SQL Server in Ihrer Umgebung installiert ist, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von SQL Server-Datenbanken verwenden.

Sie können die folgenden Aufgaben ausführen, die Sicherungsvorgänge, Wiederherstellungsvorgänge und Klonvorgänge von SQL Server-Datenbanken und Datenbankressourcen unterstützen:

- Sichern Sie SQL Server-Datenbanken und zugehörige Transaktionsprotokolle

Sie können keine Protokollsicherung für Master- und MSDB-Systemdatenbanken erstellen. Sie können jedoch Protokollsicherungen für die Modellsystemdatenbank erstellen.
- Wiederherstellen von Datenbankressourcen
  - Sie können Mastersystemdatenbanken, msdb-Systemdatenbanken und Modellsystemdatenbanken wiederherstellen.
  - Sie können nicht mehrere Datenbanken, Instanzen und Verfügbarkeitsgruppen wiederherstellen.
  - Sie können die Systemdatenbank nicht auf einem alternativen Pfad wiederherstellen.
- Erstellen Sie zeitpunktbezogene Klone von Produktionsdatenbanken

Sie können keine Sicherungs-, Wiederherstellungs-, Klon- und Lebenszyklusvorgänge für Tempdb-Systemdatenbanken durchführen.

- Überprüfen Sie Sicherungsvorgänge sofort oder verschieben Sie die Überprüfung auf einen späteren Zeitpunkt.

Die Überprüfung der SQL Server-Systemdatenbank wird nicht unterstützt. SnapCenter kloniert die Datenbanken, um einen Überprüfungsvorgang durchzuführen. SnapCenter kann SQL Server-Systemdatenbanken nicht klonen und daher wird die Überprüfung dieser Datenbanken nicht unterstützt.

- Planen Sie Sicherungsvorgänge und Klonvorgänge
- Überwachen von Sicherungsvorgängen, Wiederherstellungsvorgängen und Klonvorgängen



Das Plug-in für SQL Server unterstützt keine Sicherung und Wiederherstellung von SQL Server-Datenbanken auf SMB-Freigaben.

## SnapCenter Plug-in für Microsoft SQL Server-Funktionen

Das Plug-in für SQL Server lässt sich in Microsoft SQL Server auf dem Windows-Host und in die NetApp Snapshot-Technologie auf dem Speichersystem integrieren. Um mit dem Plug-in für SQL Server zu arbeiten, verwenden Sie die SnapCenter Schnittstelle.

Das Plug-in für SQL Server umfasst die folgenden Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche mit SnapCenter**

Die SnapCenter Schnittstelle bietet Ihnen Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs- und Wiederherstellungsprozesse über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen. SnapCenter bietet außerdem eine zentrale Planung und Richtlinienverwaltung zur Unterstützung von Sicherungs- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

Sie können routinemäßige SQL Server-Sicherungen planen, die richtlinienbasierte Aufbewahrung von Sicherungen konfigurieren und zeitpunktbezogene und minutengenaue Wiederherstellungsvorgänge einrichten. Sie können Ihre SQL Server-Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Technologie**

Das Plug-in für SQL Server verwendet die NetApp Snapshot-Technologie mit dem NetApp SnapCenter Plug-in für Microsoft Windows. Auf diese Weise können Sie Datenbanken in Sekundenschnelle sichern und schnell wiederherstellen, ohne SQL Server offline zu nehmen. Snapshots verbrauchen nur minimalen Speicherplatz.

Zusätzlich zu diesen Hauptfunktionen bietet das Plug-in für SQL Server die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs-, Klon- und Überprüfungs-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung
- Erstellung platzsparender Point-in-Time-Kopien von Produktionsdatenbanken zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem sich der Klon befindet, ist eine FlexClone -Lizenz erforderlich.

- Unterbrechungsfreie und automatisierte Backup-Verifizierung
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Servern auszuführen
- PowerShell-Cmdlets zum Skripting von Sicherungs-, Überprüfungs-, Wiederherstellungs- und Klonvorgängen
- Unterstützung für AlwaysOn-Verfügbarkeitsgruppen (AGs) in SQL Server zur Beschleunigung der Einrichtung, Sicherung und Wiederherstellung von AGs
- In-Memory-Datenbank und Buffer Pool Extension (BPE) als Teil von SQL Server 2014
- Unterstützung für die Sicherung von LUNs und virtuellen Maschinenfestplatten (VMDKs)
- Unterstützung für physische und virtualisierte Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM) und VMDK über NFS und VMFS



NAS-Volumes sollten über eine Standardexportrichtlinie in der Storage Virtual Machine (SVM) verfügen.

- Unterstützung für FileStream und Dateigruppen in eigenständigen SQL Server-Datenbanken.
- Unterstützung für Non-Volatile Memory Express (NVMe) auf Windows Server 2022
  - Sicherungs-, Wiederherstellungs-, Klon- und Überprüfungs-Workflows auf VMDK-Layout, das auf NVMe über TCP/IP erstellt wurde.
  - Unterstützt NVMe-Firmwareversion 1.3 ab ESX 8.0 Update 2 und erfordert virtuelle Hardwareversion 21.
  - Windows Server Failover Clustering (WSFC) wird für Anwendungen über VMDK auf NVMe über TCP/IP nicht unterstützt.
- Unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie transparent ausfallen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

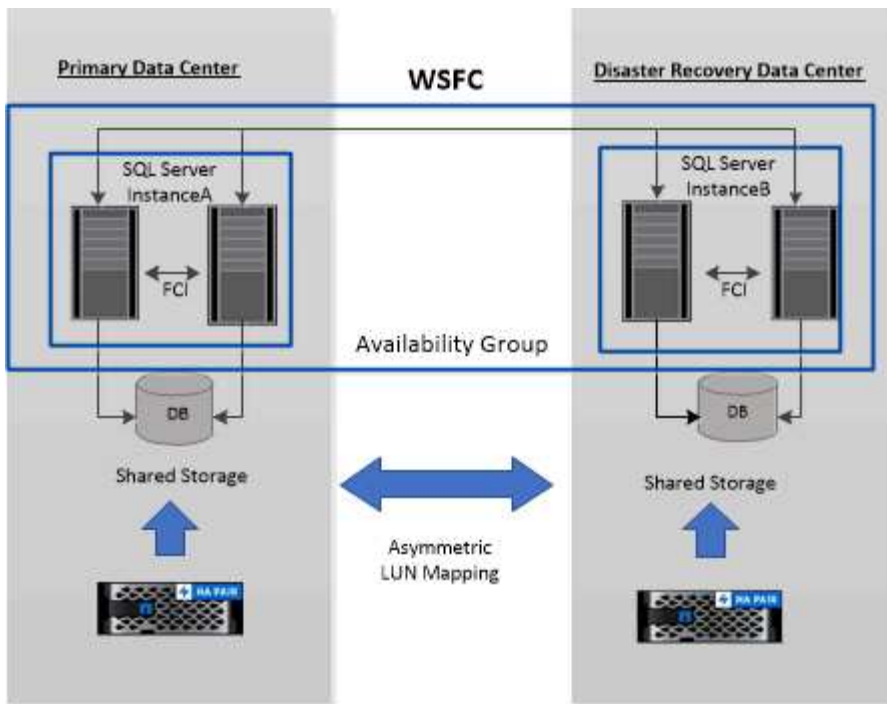
## Unterstützung für asymmetrische LUN-Zuordnung in Windows-Clustern

Das SnapCenter -Plug-in für Microsoft SQL Server unterstützt die Erkennung in SQL Server 2012 und höher, ALM-Konfigurationen (Asymmetric LUN Mapping) für hohe Verfügbarkeit und Verfügbarkeitsgruppen für die Notfallwiederherstellung. Beim Erkennen von Ressourcen erkennt SnapCenter Datenbanken auf lokalen Hosts und auf Remote-Hosts in ALM-Konfigurationen.

Eine ALM-Konfiguration ist ein einzelner Windows-Server-Failovercluster, der einen oder mehrere Knoten in einem primären Rechenzentrum und einen oder mehrere Knoten in einem Notfallwiederherstellungszentrum enthält.

Nachfolgend sehen Sie ein Beispiel für eine ALM-Konfiguration:

- Zwei Failovercluster-Instanzen (FCI) in einem Rechenzentrum mit mehreren Standorten
- FCI für lokale Hochverfügbarkeit (HA) und Verfügbarkeitsgruppe (AG) für Notfallwiederherstellung mit einer eigenständigen Instanz am Notfallwiederherstellungsstandort



#### WSFC----Windows Server Failover Cluster

Der Speicher im primären Rechenzentrum wird zwischen den im primären Rechenzentrum vorhandenen FCI-Knoten gemeinsam genutzt. Der Speicher im Notfallwiederherstellungs-Rechenzentrum wird zwischen den im Notfallwiederherstellungs-Rechenzentrum vorhandenen FCI-Knoten gemeinsam genutzt.

Der Speicher im primären Rechenzentrum ist für die Knoten im Notfallwiederherstellungs-Rechenzentrum nicht sichtbar und umgekehrt.

Die ALM-Architektur kombiniert zwei gemeinsam genutzte Speicherlösungen, die von FCI verwendet werden, mit einer nicht gemeinsam genutzten oder dedizierten Speicherlösung, die von SQL AG verwendet wird. Die AG-Lösung verwendet identische Laufwerksbuchstaben für gemeinsam genutzte Festplattenressourcen in allen Rechenzentren. Diese Speicheranordnung, bei der eine Clusterfestplatte von einer Teilmenge von Knoten innerhalb eines WSFC gemeinsam genutzt wird, wird als ALM bezeichnet.

### Vom SnapCenter Plug-in für Microsoft SQL Server unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen als auch auf virtuellen Maschinen. Sie müssen überprüfen, ob für Ihren Speichertyp Unterstützung verfügbar ist, bevor Sie das Paket für Ihren Host installieren.

SnapCenter -Bereitstellungs- und Datenschutzunterstützung ist auf Windows Server verfügbar. Die neuesten Informationen zu unterstützten Versionen finden Sie im [https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp Interoperabilitätsmatrix-Tool\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\) .

| <b>Maschine</b>   | <b>Speichertyp</b>                                                                    | <b>Bereitstellung mittels</b>                                             | <b>Support-Hinweise</b>             |
|-------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------|
| Physischer Server | FC-verbundene LUNs                                                                    | Grafische Benutzeroberfläche (GUI) von SnapCenter oder PowerShell-Cmdlets |                                     |
| Physischer Server | Über iSCSI verbundene LUNs                                                            | SnapCenter -GUI oder PowerShell-Cmdlets                                   |                                     |
| Physischer Server | SMB3 (CIFS)-Freigaben auf einer Storage Virtual Machine (SVM)                         | SnapCenter -GUI oder PowerShell-Cmdlets                                   | Support nur für die Bereitstellung. |
| VMware VM         | Über einen FC- oder iSCSI-HBA verbundene RDM-LUNs                                     | PowerShell-Cmdlets                                                        |                                     |
| VMware VM         | iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind          | SnapCenter -GUI oder PowerShell-Cmdlets                                   |                                     |
| VMware VM         | Virtual Machine File Systems (VMFS) oder NFS-Datenspeicher                            | VMware vSphere                                                            |                                     |
| VMware VM         | Ein Gastsystem, das mit SMB3-Freigaben verbunden ist, die sich auf einer SVM befinden | SnapCenter -GUI oder PowerShell-Cmdlets                                   | Support nur für die Bereitstellung. |
| VMware VM         | vVol-Datenspeicher auf NFS und SAN                                                    | ONTAP Tools für VMware vSphere                                            |                                     |

| Maschine   | Speichertyp                                                                             | Bereitstellung mittels                  | Support-Hinweise                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hyper-V-VM | Virtuelle FC (vFC) LUNs, die durch einen virtuellen Fibre Channel Switch verbunden sind | SnapCenter -GUI oder PowerShell-Cmdlets | <p>Sie müssen Hyper-V Manager verwenden, um Virtual FC (vFC)-LUNs bereitzustellen, die über einen virtuellen Fibre Channel-Switch verbunden sind.</p> <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div> |
| Hyper-V-VM | iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind            | SnapCenter -GUI oder PowerShell-Cmdlets | <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div>                                                                                                                                                     |

| Maschine   | Speichertyp                                                                           | Bereitstellung mittels                  | Support-Hinweise                                                                                                                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hyper-V-VM | Ein Gastsystem, das mit SMB3-Freigaben verbunden ist, die sich auf einer SVM befinden | SnapCenter -GUI oder PowerShell-Cmdlets | <p>Support nur für die Bereitstellung.</p> <p> Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> |

## Empfehlungen zum Speicherlayout für das SnapCenter -Plug-in für Microsoft SQL Server

Ein gut konzipiertes Speicherlayout ermöglicht es SnapCenter Server, Ihre Datenbanken zu sichern, um Ihre Wiederherstellungsziele zu erreichen. Beim Definieren Ihres Speicherlayouts sollten Sie mehrere Faktoren berücksichtigen, darunter die Größe der Datenbank, die Änderungsrate der Datenbank und die Häufigkeit, mit der Sie Sicherungen durchführen.

In den folgenden Abschnitten werden die Empfehlungen und Einschränkungen zum Speicherlayout für LUNs und virtuelle Maschinendatenträger (VMDKs) mit dem in Ihrer Umgebung installierten SnapCenter Plug-in für Microsoft SQL Server definiert.

In diesem Fall können LUNs VMware RDM-Festplatten und direkt angeschlossene iSCSI-LUNs umfassen, die dem Gast zugeordnet sind.

### LUN- und VMDK-Anforderungen

Sie können optional dedizierte LUNs oder VMDKs für optimale Leistung und Verwaltung für die folgenden Datenbanken verwenden:

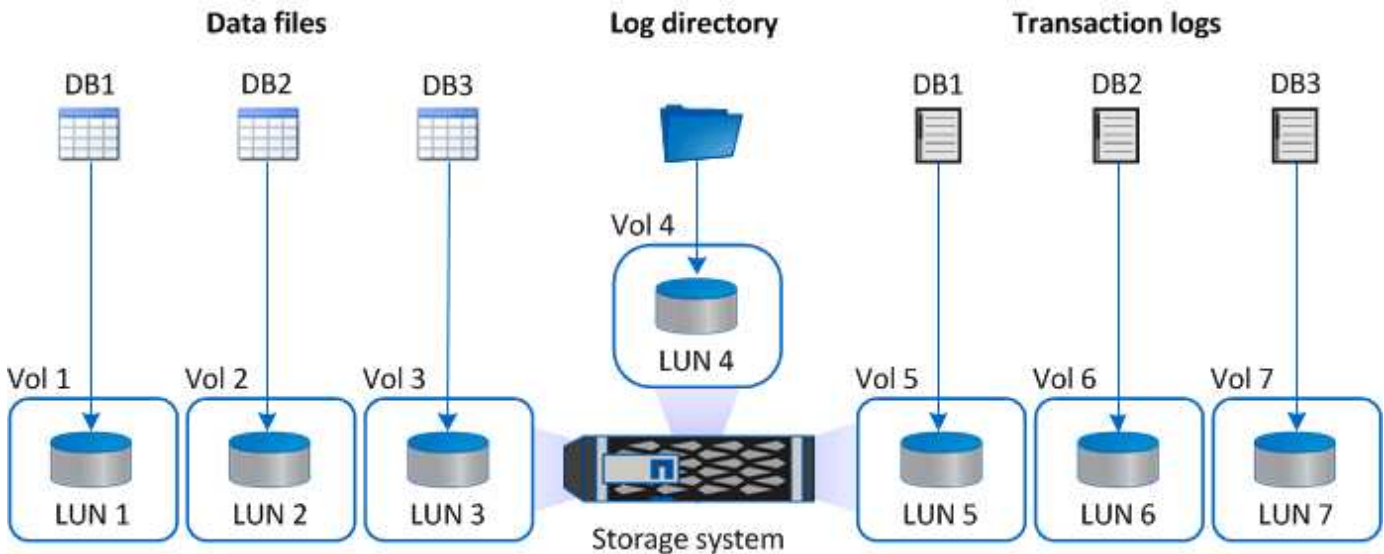
- Master- und Modellsystemdatenbanken
- Tempdb
- Benutzerdatenbankdateien (.mdf und .ndf)
- Transaktionsprotokolldateien der Benutzerdatenbank (.ldf)
- Protokollverzeichnis

Zum Wiederherstellen großer Datenbanken empfiehlt es sich, dedizierte LUNs oder VMDKs zu verwenden. Die Wiederherstellung einer vollständigen LUN oder VMDK dauert kürzer als die Wiederherstellung der einzelnen Dateien, die in der LUN oder VMDK gespeichert sind.

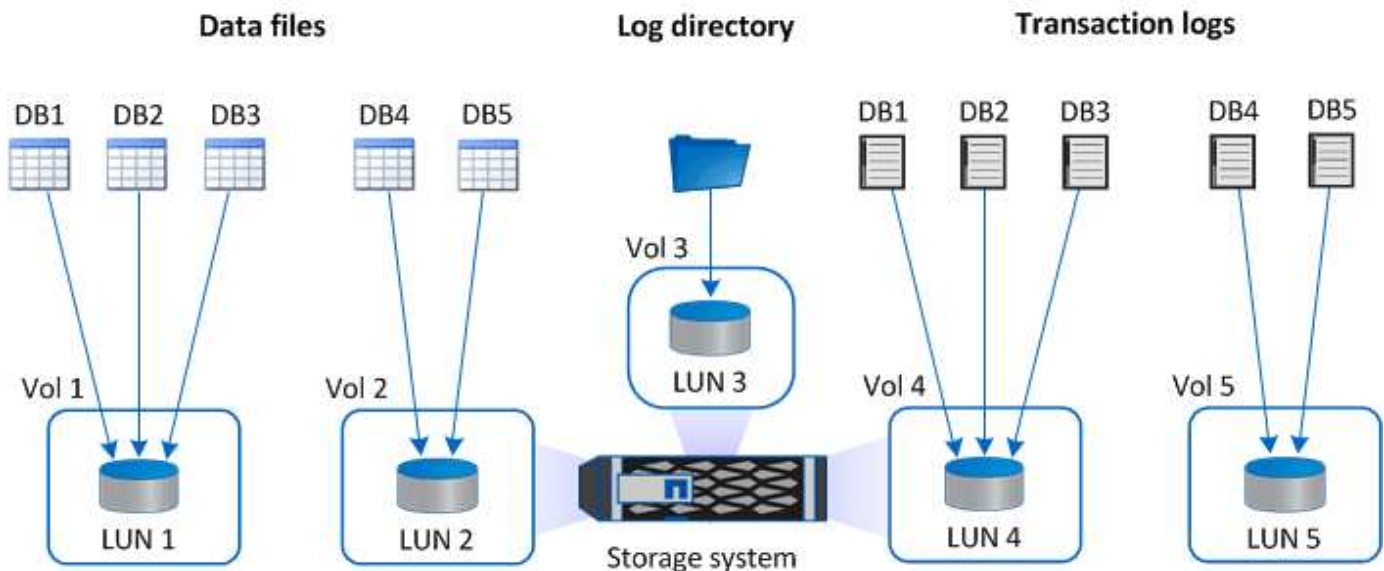
Für das Protokollverzeichnis sollten Sie eine separate LUN oder VMDK erstellen, damit auf den Datenträgern für die Daten oder Protokolldateien ausreichend freier Speicherplatz vorhanden ist.

### LUN- und VMDK-Beispiellayouts

Die folgende Grafik zeigt, wie Sie das Speicherlayout für große Datenbanken auf LUNs konfigurieren können:

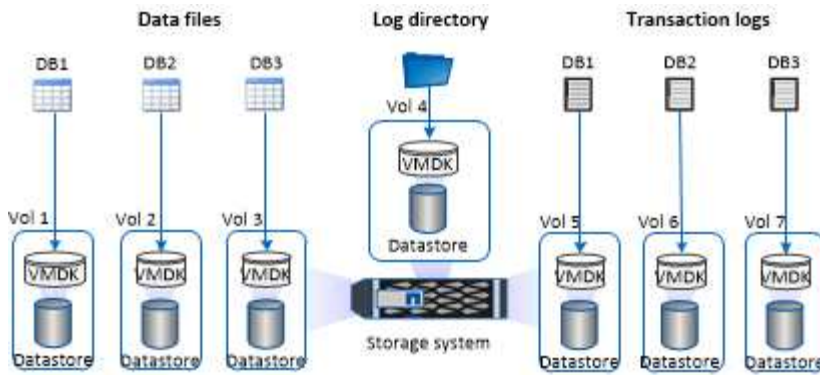


Die folgende Grafik zeigt, wie Sie das Speicherlayout für mittlere oder kleine Datenbanken auf LUNs konfigurieren können:

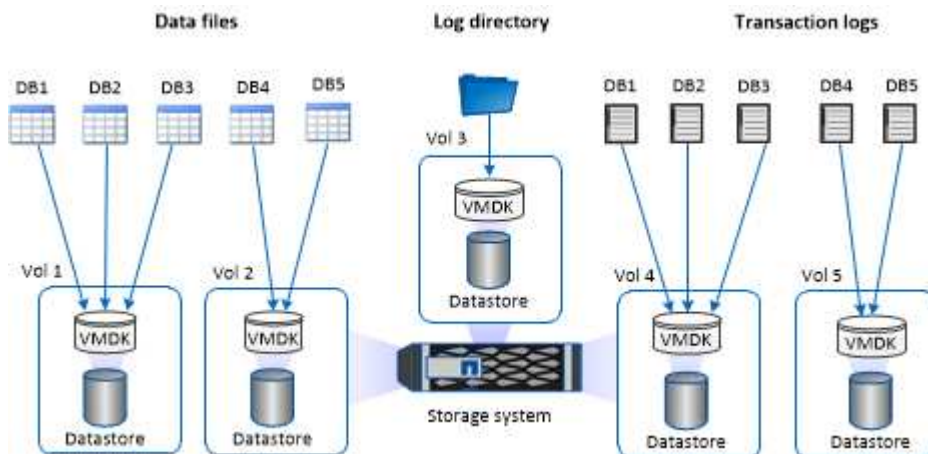


Die folgende Grafik zeigt, wie Sie das Speicherlayout für große Datenbanken auf VMDKs konfigurieren können:





Die folgende Grafik zeigt, wie Sie das Speicherlayout für mittlere oder kleine Datenbanken auf VMDKs konfigurieren können:



## Für das SQL-Plug-In sind mindestens ONTAP Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN löschen
  - lun igroup hinzufügen
  - lun igroup erstellen
  - LUN-Igroup löschen
  - LUN-Igroup umbenennen
  - lun igroup show
  - LUN-Zuordnung Add-Reporting-Nodes
  - LUN-Zuordnung erstellen

- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung

- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Netzwerkschnittstelle
- Netzwerkschnittstelle anzeigen
- vServer
- Metrocluster-Show

## **Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für das Plug-in für SQL Server vor**

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#) .

## Sicherungsstrategie für SQL Server-Ressourcen

### Definieren einer Sicherungsstrategie für SQL Server-Ressourcen

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge können Sie sicherstellen, dass Sie über die Sicherungen verfügen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Datenbanken benötigen. Ihre Sicherungsstrategie wird weitgehend von Ihrem Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmt.

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Die RTO ist die Zeit, bis zu der ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt sein muss. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Backup-Strategie bei.

### Unterstützte Sicherungstypen

Zum Sichern von SQL Server-System- und Benutzerdatenbanken mit SnapCenter müssen Sie den Ressourcentyp auswählen, z. B. Datenbanken, SQL Server-Instanzen und Verfügbarkeitsgruppen (AG). Mithilfe der Snapshot-Technologie werden schreibgeschützte Onlinekopien der Volumes erstellt, auf denen sich die Ressourcen befinden.

Sie können die Option „Nur kopieren“ auswählen, um anzugeben, dass der SQL Server Transaktionsprotokolle nicht abschneidet. Sie sollten diese Option verwenden, wenn Sie den SQL Server auch mit anderen Sicherungsanwendungen verwalten. Wenn die Transaktionsprotokolle intakt bleiben, kann jede Sicherungsanwendung die Systemdatenbanken wiederherstellen. Nur-Kopier-Backups sind unabhängig von der Reihenfolge der geplanten Backups und haben keinen Einfluss auf die Backup- und Wiederherstellungsvorgänge der Datenbank.

| <b>Sicherungstyp</b>                          | <b>Beschreibung</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Nur-Kopier-Option mit Sicherungstyp</b>                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vollständige Sicherung und Protokollsicherung | <p>Sichert die Systemdatenbank und kürzt die Transaktionsprotokolle.</p> <p>Der SQL Server kürzt die Transaktionsprotokolle, indem er die Einträge entfernt, die bereits in der Datenbank festgeschrieben sind.</p> <p>Nach Abschluss der vollständigen Sicherung wird mit dieser Option ein Transaktionsprotokoll erstellt, in dem Transaktionsinformationen erfasst werden. Normalerweise sollten Sie diese Option wählen. Wenn Ihre Sicherungszeit jedoch kurz ist, können Sie bei einer vollständigen Sicherung auf die Ausführung einer Transaktionsprotokollsicherung verzichten.</p> <p>Sie können keine Protokollsicherung für Master- und MSDB-Systemdatenbanken erstellen. Sie können jedoch Protokollsicherungen für die Modellsystemdatenbank erstellen.</p> | <p>Sichert die Systemdatenbankdateien und die Transaktionsprotokolle, ohne die Protokolle abzuschneiden.</p> <p>Eine reine Kopiesicherung kann nicht als differenzielle Basis oder differenzielle Sicherung dienen und hat keinen Einfluss auf die differenzielle Basis. Das Wiederherstellen einer vollständigen Nur-Kopier-Sicherung ist dasselbe wie das Wiederherstellen jeder anderen vollständigen Sicherung.</p> |
| Vollständige Datenbanksicherung               | <p>Sichert die Systemdatenbankdateien.</p> <p>Sie können eine vollständige Datenbanksicherung für Master-, Modell- und MSDB-Systemdatenbanken erstellen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Sichert die Systemdatenbankdateien.                                                                                                                                                                                                                                                                                                                                                                                     |

| Sicherungstyp                  | Beschreibung                                                                                                                                                                                                                                                                                                                                     | Nur-Kopier-Option mit Sicherungstyp                                                                                                                                                                                                                                               |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transaktionsprotokollsicherung | <p>Sichert die gekürzten Transaktionsprotokolle und kopiert nur die Transaktionen, die seit der Sicherung des letzten Transaktionsprotokolls festgeschrieben wurden.</p> <p>Wenn Sie neben vollständigen Datenbanksicherungen auch häufige Transaktionsprotokollsicherungen planen, können Sie granulare Wiederherstellungspunkte auswählen.</p> | <p>Sichert die Transaktionsprotokolle, ohne sie zu kürzen.</p> <p>Dieser Sicherungstyp hat keinen Einfluss auf die Reihenfolge der regulären Protokollsicherungen. Nur-Kopier-Protokollsicherungen sind für die Durchführung von Online-Wiederherstellungsvorgängen nützlich.</p> |

### Sicherungszeitpläne für Plug-in für SQL Server

Die Sicherungshäufigkeit (Zeitplantyp) wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen. Beispielsweise können regelmäßige Sicherungen des Transaktionsprotokolls ausreichen, um sicherzustellen, dass Sie über die erforderlichen Sicherungen verfügen. Je häufiger Sie Ihre Datenbanken sichern, desto weniger Transaktionsprotokolle muss SnapCenter zum Zeitpunkt der Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können als Sicherungshäufigkeit für die Richtlinie stündlich, täglich, wöchentlich oder monatlich auswählen. Wenn Sie keine dieser Frequenzen auswählen, handelt es sich bei der erstellten Richtlinie um eine Nur-On-Demand-Richtlinie. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen > Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen > Ressourcengruppen** klicken.

### Anzahl der für Datenbanken benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Datenbank, die Anzahl der verwendeten Volumes, die Änderungsrate der Datenbank und Ihr Service Level Agreement (SLA).

Bei Datenbanksicherungen hängt die Anzahl der von Ihnen ausgewählten Sicherungsaufträge normalerweise von der Anzahl der Datenträger ab, auf denen Sie Ihre Datenbanken platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Datenbanken auf einem Volume und eine große Datenbank auf einem anderen Volume platziert haben, können Sie einen Sicherungsauftrag für die kleinen Datenbanken und einen Sicherungsauftrag für die große Datenbank erstellen.

### Sicherungsnamenskonventionen für Plug-in für SQL Server

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: `customtext_resourcegroup_policy_hostname` oder `resourcegroup_hostname`. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

### Sicherungsaufbewahrungsoptionen für Plug-in für SQL Server

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise

kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.



Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

### **Wie lange sollen Transaktionsprotokollsicherungen auf dem Quellspeichersystem aufbewahrt werden?**

Das SnapCenter Plug-in für Microsoft SQL Server benötigt Transaktionsprotokollsicherungen, um aktuelle Wiederherstellungsvorgänge durchzuführen, die Ihre Datenbank auf einen Zeitpunkt zwischen zwei vollständigen Sicherungen wiederherstellen.

Wenn Plug-in für SQL Server beispielsweise um 8:00 Uhr eine vollständige Sicherung und um 17:00 Uhr eine weitere vollständige Sicherung erstellt hat, kann es die neueste Transaktionsprotokollsicherung verwenden, um die Datenbank auf einen beliebigen Zeitpunkt zwischen 8:00 Uhr und 17:00 Uhr wiederherzustellen. Wenn keine Transaktionsprotokolle verfügbar sind, kann Plug-in für SQL Server nur zeitpunktbezogene Wiederherstellungsvorgänge durchführen, die eine Datenbank auf den Zeitpunkt wiederherstellen, zu dem Plug-in für SQL Server eine vollständige Sicherung abgeschlossen hat.

Normalerweise benötigen Sie aktuelle Wiederherstellungsvorgänge nur für ein oder zwei Tage. Standardmäßig behält SnapCenter mindestens zwei Tage.

### **Mehrere Datenbanken auf demselben Volume**

Sie können alle Datenbanken auf demselben Datenträger ablegen, da die Sicherungsrichtlinie eine Option zum Festlegen der maximalen Anzahl von Datenbanken pro Sicherung enthält (Standardwert ist 100).

Wenn Sie beispielsweise 200 Datenbanken im selben Volume haben, werden zwei Snapshots mit jeweils 100 Datenbanken in den beiden Snapshots erstellt.

### **Überprüfung der Sicherungskopie mithilfe des primären oder sekundären Speichervolumens für Plug-in für SQL Server**

Sie können Sicherungskopien auf dem primären Speichervolume oder auf dem sekundären Speichervolume von SnapMirror oder SnapVault überprüfen. Durch die Überprüfung mithilfe eines sekundären Speichervolumens wird die Belastung des primären Speichervolumens reduziert.

Wenn Sie eine Sicherung überprüfen, die sich entweder auf dem primären oder sekundären Speichervolume



befindet, werden alle primären und sekundären Snapshots als überprüft markiert.

Zum Überprüfen von Sicherungskopien auf dem sekundären Speichervolume von SnapMirror und SnapVault ist eine SnapRestore -Lizenz erforderlich.

### **Wann sollten Überprüfungsjobs geplant werden?**

Obwohl SnapCenter Backups unmittelbar nach der Erstellung überprüfen kann, kann dies die zum Abschließen des Backup-Auftrags erforderliche Zeit erheblich verlängern und ist ressourcenintensiv. Daher ist es fast immer am besten, die Überprüfung in einem separaten Job für einen späteren Zeitpunkt einzuplanen. Wenn Sie beispielsweise täglich um 17:00 Uhr eine Datenbank sichern, können Sie die Überprüfung eine Stunde später um 18:00 Uhr planen.

Aus demselben Grund ist es normalerweise nicht notwendig, bei jeder Sicherung eine Sicherungsüberprüfung durchzuführen. Um die Integrität der Sicherung sicherzustellen, reicht es normalerweise aus, in regelmäßigen, aber weniger häufigen Abständen eine Überprüfung durchzuführen. Ein einzelner Überprüfungsaufruf kann mehrere Sicherungen gleichzeitig überprüfen.

## **Wiederherstellungsstrategie für SQL Server**

### **Quellen und Ziele für einen Wiederherstellungsvorgang**

Sie können eine SQL Server-Datenbank aus einer Sicherungskopie auf einem primären oder sekundären Speicher wiederherstellen. Sie können die Datenbank zusätzlich zu ihrem ursprünglichen Speicherort auch an anderen Zielen wiederherstellen und so das Ziel auswählen, das Ihren Anforderungen entspricht.

#### **Quellen für einen Wiederherstellungsvorgang**

Sie können Datenbanken vom primären oder sekundären Speicher wiederherstellen.

#### **Ziele für einen Wiederherstellungsvorgang**

Sie können Datenbanken an verschiedenen Zielen wiederherstellen:

| <b>Ziel</b>                                                                  | <b>Beschreibung</b>                                                                                                                                        |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Der ursprüngliche Standort                                                   | Standardmäßig stellt SnapCenter die Datenbank am selben Speicherort auf derselben SQL Server-Instanz wieder her.                                           |
| Ein anderer Standort                                                         | Sie können die Datenbank an einem anderen Speicherort auf einer beliebigen SQL Server-Instanz innerhalb desselben Hosts wiederherstellen.                  |
| Ursprünglicher oder anderer Speicherort mit unterschiedlichen Datenbanknamen | Sie können die Datenbank unter einem anderen Namen auf jeder SQL Server-Instanz auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde. |



Die Wiederherstellung auf einem alternativen Host über ESX-Server für SQL-Datenbanken auf VMDKs (NFS- und VMFS-Datenspeicher) wird nicht unterstützt.

## Von SnapCenter unterstützte SQL Server-Wiederherstellungsmodelle

Jedem Datenbanktyp werden standardmäßig bestimmte Wiederherstellungsmodelle zugewiesen. Der SQL Server-Datenbankadministrator kann jeder Datenbank ein anderes Wiederherstellungsmodell zuweisen.

SnapCenter unterstützt drei Arten von SQL Server-Wiederherstellungsmodellen:

- Einfaches Wiederherstellungsmodell

Wenn Sie das einfache Wiederherstellungsmodell verwenden, können Sie die Transaktionsprotokolle nicht sichern.

- Vollständiges Wiederherstellungsmodell

Wenn Sie das vollständige Wiederherstellungsmodell verwenden, können Sie eine Datenbank ab dem Fehlerpunkt in ihren vorherigen Zustand wiederherstellen.

- Massenprotokolliertes Wiederherstellungsmodell

Wenn Sie das massenprotokollierte Wiederherstellungsmodell verwenden, müssen Sie den massenprotokollierten Vorgang manuell erneut ausführen. Sie müssen den Massenprotokollierungsvorgang ausführen, wenn das Transaktionsprotokoll, das den Commit-Datensatz des Vorgangs enthält, vor der Wiederherstellung nicht gesichert wurde. Wenn durch den massenprotokollierten Vorgang 10 Millionen Zeilen in eine Datenbank eingefügt werden und die Datenbank ausfällt, bevor das Transaktionsprotokoll gesichert wird, enthält die wiederhergestellte Datenbank nicht die Zeilen, die durch den massenprotokollierten Vorgang eingefügt wurden.

## Arten von Wiederherstellungsvorgängen

Sie können SnapCenter verwenden, um verschiedene Arten von Wiederherstellungsvorgängen an SQL Server-Ressourcen durchzuführen.

- Aktuelle Wiederherstellung
- Wiederherstellen eines früheren Zeitpunkts

In den folgenden Situationen können Sie die Daten auf die Minute genau wiederherstellen oder zu einem früheren Zeitpunkt wiederherstellen:

- Wiederherstellung vom SnapMirror oder SnapVault Sekundärspeicher
- Auf alternativem Pfad (Speicherort) wiederherstellen



SnapCenter unterstützt kein volumenbasiertes SnapRestore.

## Wiederherstellung auf die Minute genau

Bei einem minutengenauen Wiederherstellungsvorgang (standardmäßig ausgewählt) werden Datenbanken bis zum Fehlerpunkt wiederhergestellt. SnapCenter erreicht dies durch Ausführen der folgenden Sequenz:

1. Sichert das letzte aktive Transaktionsprotokoll, bevor die Datenbank wiederhergestellt wird.
2. Stellt die Datenbanken aus der von Ihnen ausgewählten vollständigen Datenbanksicherung wieder her.
3. Wendet alle Transaktionsprotokolle an, die nicht in die Datenbanken übernommen wurden (einschließlich Transaktionsprotokolle aus den Sicherungen vom Zeitpunkt der Erstellung der Sicherung bis zum aktuellsten Zeitpunkt).

Transaktionsprotokolle werden weitergeleitet und auf alle ausgewählten Datenbanken angewendet.

Für einen minutengenauen Wiederherstellungsvorgang ist ein zusammenhängender Satz von Transaktionsprotokollen erforderlich.

Da SnapCenter SQL Server-Datenbanktransaktionsprotokolle nicht aus Protokollversand-Sicherungsdateien wiederherstellen kann (Protokollversand ermöglicht Ihnen das automatische Senden von Transaktionsprotokollsicherungen von einer primären Datenbank auf einer primären Serverinstanz an eine oder mehrere sekundäre Datenbanken auf separaten sekundären Serverinstanzen), können Sie keinen minutenaktuellen Wiederherstellungsvorgang aus den Transaktionsprotokollsicherungen durchführen. Aus diesem Grund sollten Sie das SnapCenter verwenden, um die Transaktionsprotokolldateien Ihrer SQL Server-Datenbank zu sichern.

Wenn Sie nicht für alle Sicherungen die Wiederherstellungsfunktion auf die Minute genau benötigen, können Sie die Aufbewahrungsdauer der Transaktionsprotokollsicherungen Ihres Systems über die Sicherungsrichtlinien konfigurieren.

#### **Beispiel für einen minutengenauen Wiederherstellungsvorgang**

Angenommen, Sie führen die SQL Server-Sicherung jeden Tag mittags aus und müssen am Mittwoch um 16:00 Uhr eine Wiederherstellung aus einer Sicherung durchführen. Aus irgendeinem Grund ist die Überprüfung der Sicherung vom Mittwochmittag fehlgeschlagen, daher entscheiden Sie sich für die Wiederherstellung aus der Sicherung vom Dienstagmittag. Wenn die Sicherung anschließend wiederhergestellt wird, werden alle Transaktionsprotokolle nach vorne verschoben und auf die wiederhergestellten Datenbanken angewendet. Dabei beginnen wir mit denen, die beim Erstellen der Sicherung vom Dienstag nicht festgeschrieben wurden, und fahren mit dem letzten Transaktionsprotokoll fort, das am Mittwoch um 16:00 Uhr geschrieben wurde (sofern die Transaktionsprotokolle gesichert wurden).

#### **Wiederherstellen eines früheren Zeitpunkts**

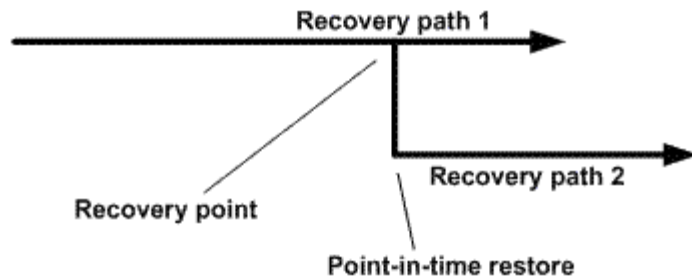
Bei einer zeitpunktbezogenen Wiederherstellung werden Datenbanken nur auf einen bestimmten Zeitpunkt in der Vergangenheit wiederhergestellt. Eine zeitpunktbezogene Wiederherstellung erfolgt in den folgenden Wiederherstellungssituationen:

- Die Datenbank wird zu einem bestimmten Zeitpunkt in einem gesicherten Transaktionsprotokoll wiederhergestellt.
- Die Datenbank wird wiederhergestellt und nur eine Teilmenge der gesicherten Transaktionsprotokolle wird darauf angewendet.



Durch die Wiederherstellung einer Datenbank zu einem bestimmten Zeitpunkt ergibt sich ein neuer Wiederherstellungspfad.

Das folgende Bild veranschaulicht die Probleme bei der Ausführung einer zeitpunktbezogenen Wiederherstellung:



Im Bild besteht Wiederherstellungspfad 1 aus einer vollständigen Sicherung, gefolgt von mehreren Transaktionsprotokollsicherungen. Sie stellen die Datenbank zu einem bestimmten Zeitpunkt wieder her. Nach der Point-in-Time-Wiederherstellung werden neue Transaktionsprotokollsicherungen erstellt, was zu Wiederherstellungspfad 2 führt. Die neuen Transaktionsprotokollsicherungen werden erstellt, ohne eine neue vollständige Sicherung zu erstellen. Aufgrund von Datenbeschädigungen oder anderen Problemen können Sie die aktuelle Datenbank erst wiederherstellen, wenn eine neue vollständige Sicherung erstellt wurde. Außerdem ist es nicht möglich, die im Wiederherstellungspfad 2 erstellten Transaktionsprotokolle auf die vollständige Sicherung anzuwenden, die zum Wiederherstellungspfad 1 gehört.

Wenn Sie Transaktionsprotokollsicherungen anwenden, können Sie auch ein bestimmtes Datum und eine bestimmte Uhrzeit angeben, zu der die Anwendung der gesicherten Transaktionen beendet werden soll. Geben Sie dazu ein Datum und eine Uhrzeit innerhalb des verfügbaren Bereichs an und das SnapCenter entfernt alle Transaktionen, die vor diesem Zeitpunkt nicht festgeschrieben wurden. Mit dieser Methode können Sie Datenbanken auf einen Zeitpunkt vor dem Auftreten einer Beschädigung zurücksetzen oder eine versehentliche Datenbank- oder Tabellenlöschung wiederherstellen.

#### Beispiel für eine zeitpunktbezogene Wiederherstellung

Angenommen, Sie führen einmal um Mitternacht eine vollständige Datenbanksicherung und stündlich eine Transaktionsprotokollsicherung durch. Die Datenbank stürzt um 9:45 Uhr ab, Sie sichern jedoch trotzdem die Transaktionsprotokolle der ausgefallenen Datenbank. Sie können zwischen diesen Point-in-Time-Wiederherstellungsszenarien wählen:

- Stellen Sie die vollständige Datenbanksicherung wieder her, die um Mitternacht erstellt wurde, und akzeptieren Sie den Verlust der danach vorgenommenen Datenbankänderungen. (Option: Keine)
- Vollständige Datenbanksicherung wiederherstellen und alle Transaktionsprotokollsicherungen bis 9:45 Uhr anwenden (Option: Protokollieren bis)
- Stellen Sie die vollständige Datenbanksicherung wieder her und wenden Sie Transaktionsprotokollsicherungen an. Geben Sie dabei den Zeitpunkt an, zu dem die Transaktionen aus dem letzten Satz von Transaktionsprotokollsicherungen wiederhergestellt werden sollen. (Option: Nach bestimmter Zeit)

In diesem Fall würden Sie das Datum und die Uhrzeit berechnen, zu der ein bestimmter Fehler gemeldet wurde. Alle Transaktionen, die nicht vor dem angegebenen Datum und der angegebenen Uhrzeit festgeschrieben wurden, werden entfernt.

## Definieren einer Klonstrategie für SQL Server

Durch die Definition einer Klonstrategie können Sie Ihre Datenbank erfolgreich klonen.

1. Überprüfen Sie die Einschränkungen im Zusammenhang mit Klonvorgängen.
2. Entscheiden Sie sich für den Klontyp, den Sie benötigen.

### Einschränkungen von Klonvorgängen

Sie sollten sich der Einschränkungen von Klonvorgängen bewusst sein, bevor Sie die Datenbanken klonen.

- Wenn Sie eine beliebige Version von Oracle zwischen 11.2.0.4 und 12.1.0.1 verwenden, bleibt der Klonvorgang hängen, wenn Sie den Befehl *renamedg* ausführen. Sie können den Oracle-Patch 19544733 anwenden, um dieses Problem zu beheben.
- Das Klonen von Datenbanken von einer LUN, die direkt an einen Host angeschlossen ist (z. B. mithilfe des Microsoft iSCSI-Initiators auf einem Windows-Host), auf eine VMDK oder eine RDM-LUN auf demselben oder einem anderen Windows-Host oder umgekehrt wird nicht unterstützt.
- Das Stammverzeichnis des Volume-Mount-Punkts darf kein freigegebenes Verzeichnis sein.
- Wenn Sie eine LUN, die einen Klon enthält, auf ein neues Volume verschieben, kann der Klon nicht gelöscht werden.

### Arten von Klonvorgängen

Sie können SnapCenter verwenden, um entweder eine SQL Server-Datenbanksicherung oder eine Produktionsdatenbank zu klonen.

- Klonen aus einer Datenbanksicherung

Die geklonte Datenbank kann als Basis für die Entwicklung neuer Anwendungen dienen und dabei helfen, Anwendungsfehler zu isolieren, die in der Produktionsumgebung auftreten. Die geklonte Datenbank kann auch zur Wiederherstellung nach leichten Datenbankfehlern verwendet werden.

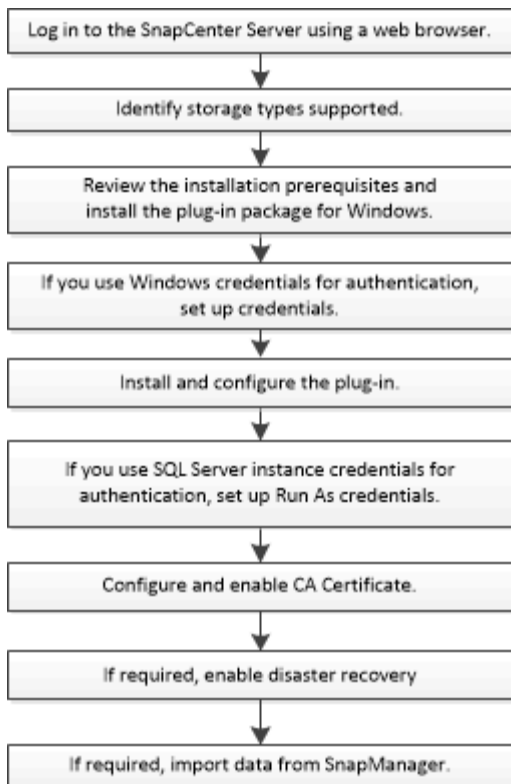
- Lebenszyklus des Klons

Sie können SnapCenter verwenden, um wiederkehrende Klonaufträge zu planen, die ausgeführt werden, wenn die Produktionsdatenbank nicht ausgelastet ist.

## Vorbereiten der Installation des SnapCenter Plug-Ins für Microsoft SQL Server

### Installationsworkflow für das SnapCenter -Plug-in für Microsoft SQL Server

Sie sollten das SnapCenter Plug-in für Microsoft SQL Server installieren und einrichten, wenn Sie SQL Server-Datenbanken schützen möchten.



## Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-Ins für Microsoft SQL Server

Bevor Sie einen Host hinzufügen und die Plug-In-Pakete installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen über einen Benutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Wenn Sie Clusterknoten in SnapCenter verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Knoten im Cluster.
- Sie müssen über einen Benutzer mit Systemadministratorberechtigungen auf dem SQL Server verfügen.

Das SnapCenter -Plug-in für Microsoft SQL Server verwendet das Microsoft VDI Framework, das Systemadministratorzugriff erfordert.

["Microsoft-Supportartikel 2926557: SQL Server VDI-Sicherungs- und Wiederherstellungsvorgänge erfordern Sysadmin-Berechtigungen"](#)

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Wenn SnapManager für Microsoft SQL Server installiert ist, müssen Sie den Dienst und die Zeitpläne gestoppt oder deaktiviert haben.

Wenn Sie Sicherungs- oder Klonaufträge in SnapCenter importieren möchten, deinstallieren Sie SnapManager für Microsoft SQL Server nicht.

- Der Host muss vom Server aus in den vollqualifizierten Domännennamen (FQDN) auflösbar sein.

Wenn die Hosts-Datei geändert wird, um sie auflösbar zu machen, und wenn sowohl der Kurzname als auch der FQDN in der Hosts-Datei angegeben sind, erstellen Sie einen Eintrag in der SnapCenter Hosts-Datei im folgenden Format: <IP-Adresse> <Host-FQDN> <Hostname>

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a>.</p>                                                                                                                                                                                                                                                                                                                                           |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>5 GB</p> <div>  <p>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.</p> </div> |

| Artikel                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Erforderliche Softwarepakete | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java und OpenJDK</li> </ul> <p>Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

## Einrichten der Anmeldeinformationen für das SnapCenter Plug-Ins-Paket für Windows

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Datenbanken oder Windows-Dateisystemen erstellen.

### Bevor Sie beginnen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.
- Sie müssen die Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.
- SQL-Authentifizierung auf Windows-Hosts

Sie müssen nach der Installation der Plug-Ins SQL-Anmeldeinformationen einrichten.

Wenn Sie das SnapCenter -Plug-in für Microsoft SQL Server bereitstellen, müssen Sie nach der Installation der Plug-ins SQL-Anmeldeinformationen einrichten. Richten Sie Anmeldeinformationen für einen Benutzer mit SQL Server-Sysadmin-Berechtigungen ein.

Die SQL-Authentifizierungsmethode authentifiziert sich gegenüber einer SQL Server-Instanz. Dies bedeutet, dass in SnapCenter eine SQL Server-Instanz erkannt werden muss. Daher müssen Sie vor dem Hinzufügen von SQL-Anmeldeinformationen einen Host hinzufügen, Plug-In-Pakete installieren und Ressourcen aktualisieren. Sie benötigen eine SQL Server-Authentifizierung, um Vorgänge wie das Planen oder Ermitteln von Ressourcen auszuführen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die zum Konfigurieren der Anmeldeinformationen



erforderlichen Informationen an:

| Für dieses Feld...      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Benutzername/Passwort   | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"><li>• Domänenadministrator</li></ul> <p>Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"><li>◦ NetBIOS\UserName</li><li>◦ Domain FQDN\UserName</li></ul> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: UserName</p> <p>Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (&lt;) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als &lt;!10, kleiner als 10 &lt;!, Backtick `12.</p> |
| Authentifizierungsmodus | Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten. Wenn Sie den SQL-Authentifizierungsmodus auswählen, müssen Sie auch die SQL-Serverinstanz und den Host angeben, auf dem sich die SQL-Instanz befindet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

## Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource

Sie können Anmeldeinformationen konfigurieren, um für jeden Benutzer Datenschutzaufträge auf einzelnen SQL Server-Ressourcen auszuführen. Sie können die Anmeldeinformationen zwar global konfigurieren, möchten dies jedoch möglicherweise nur für eine bestimmte Ressource tun.

### Informationen zu diesem Vorgang

- Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie Ihre Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.

Wenn Sie jedoch eine SQL Server-Instanz zur Authentifizierung verwenden, müssen Sie die Anmeldeinformationen nach der Installation der Plug-Ins hinzufügen.

- Wenn Sie beim Einrichten der Anmeldeinformationen die SQL-Authentifizierung aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Vorhängeschlosssymbol angezeigt.

Wenn das Vorhängeschlosssymbol angezeigt wird, müssen Sie die Anmeldeinformationen der Instanz oder Datenbank angeben, um die Instanz oder Datenbank erfolgreich zu einer Ressourcengruppe hinzuzufügen.

- Sie müssen die Anmeldeinformationen einem rollenbasierten Zugriffssteuerungsbenutzer (RBAC) ohne Systemadministratorzugriff zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Die Anmeldeinformationen werden einer SQL-Instanz zugewiesen.
  - Die SQL-Instanz oder der Host wird einem RBAC-Benutzer zugewiesen.

Der Benutzer muss sowohl über die Ressourcengruppen- als auch über die Sicherungsberechtigung verfügen.

### Schritt 1: Anmeldeinformationen hinzufügen und konfigurieren

1. Wählen Sie im linken Navigationsbereich **Einstellungen** aus.
2. Wählen Sie auf der Seite „Einstellungen“ **Anmeldeinformationen** aus.
  - a. Um neue Anmeldeinformationen hinzuzufügen, wählen Sie **Neu**.
  - b. Konfigurieren Sie auf der Seite „Anmeldeinformationen“ die Anmeldeinformationen:

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |

| Für dieses Feld...          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername                | <p>Geben Sie den Benutzernamen ein, der für die SQL Server-Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe. Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Gültige Formate für das Feld <b>Benutzername</b> sind: <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> </ul> </li> <li>• Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur Gruppe der lokalen Administratoren gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld <b>Benutzername</b> ist: <i>Benutzername</i></li> </ul> |
| Passwort                    | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Authentifizierungsmodu<br>s | Wählen Sie den SQL Server-Authentifizierungsmodus aus. Sie können auch die Windows-Authentifizierung wählen, wenn der Windows-Benutzer über Sysadmin-Berechtigungen auf dem SQL-Server verfügt.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Gastgeber                   | Wählen Sie den Host aus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SQL Server-Instanz          | Wählen Sie die SQL Server-Instanz aus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

c. Wählen Sie **OK**, um die Anmeldeinformationen hinzuzufügen.

## Schritt 2: Instanzen konfigurieren

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Instanz“ aus.
  - a. Wählen Sie image::.../media/filter\_icon.png[Filtersymbol] und wählen Sie dann den Hostnamen aus, um die Instanzen zu filtern.
  - b. Wählen Sie image::.../media/filter\_icon.png[Filtersymbol], um den Filterbereich zu schließen.
3. Schützen Sie die Instanz auf der Seite „Instanz schützen“ und wählen Sie bei Bedarf „Anmeldeinformationen konfigurieren“ aus.

Wenn der beim SnapCenter -Server angemeldete Benutzer keinen Zugriff auf das SnapCenter Plugin für Microsoft SQL Server hat, muss der Benutzer die Anmeldeinformationen konfigurieren.



Die Anmeldeinformationsoption gilt nicht für Datenbanken und Verfügbarkeitsgruppen.

#### 4. Wählen Sie **Ressourcen aktualisieren**.

### Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

#### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

#### Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -Effectivelmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$  
.. Fügen Sie der Gruppe Computerobjekte hinzu.  
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des  
Dienstkontos.
```

#### 4. Konfigurieren Sie das gMSA auf Ihren Hosts:

- a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                   |
|---------|----------------|-----------|--------------------------------------------------|
| -----   | -----          | -----     | -----                                            |
| True    | No             | Success   | {Active Directory Domain Services,<br>Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- Starten Sie Ihren Host neu.
  - Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
  - Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
- Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
  - Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Installieren Sie das SnapCenter -Plug-in für Microsoft SQL Server

### Hosts hinzufügen und das SnapCenter Plug-Ins-Paket für Windows installieren

Sie müssen die SnapCenter -Seite **Host hinzufügen** verwenden, um Hosts hinzuzufügen und das Plug-In-Paket zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

#### Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, sollten Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

["Konfigurieren Sie ein gruppenverwaltetes Dienstkonto auf Windows Server 2016 oder höher für SQL"](#)

### Informationen zu diesem Vorgang

Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.

Sie können einen Host hinzufügen und die Plug-in-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie die Plug-Ins auf einem Cluster oder Windows Server Failover Clustering (WSFC) installieren, werden die Plug-Ins auf allen Knoten des Clusters installiert.

Informationen zum Verwalten von Hosts finden Sie unter ["Hosts verwalten"](#) .

### Schritte

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

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosttyp            | <p>Wählen Sie Windows als Hosttyp aus. Der SnapCenter -Server fügt den Host hinzu und installiert dann das Plug-in für Windows, falls das Plug-in noch nicht auf dem Host installiert ist.</p> <p>Wenn Sie auf der Plug-In-Seite die Option Microsoft SQL Server auswählen, installiert der SnapCenter -Server das Plug-In für SQL Server.</p> |

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hostname             | <p>Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. IP-Adressen werden für nicht vertrauenswürdige Domänenhosts nur unterstützt, wenn sie in den FQDN aufgelöst werden.</p> <p>SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p> <p>Sie können die IP-Adressen oder den FQDN eines der folgenden Elemente eingeben:</p> <ul style="list-style-type: none"> <li>• Eigenständiger Host</li> <li>• WSFC: Wenn Sie mithilfe von SnapCenter einen Host hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.</li> </ul>                                                                                                                             |
| Anmeldeinformationen | <p>Wählen Sie 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.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div data-bbox="873 1373 927 1430">  </div> <div data-bbox="987 1318 1409 1486"> <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

5. Wählen Sie im Abschnitt **Zu installierende Plug-ins auswählen** die zu installierenden Plug-ins aus.
6. Wählen Sie **Weitere Optionen**.

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen                                                                                       | <p>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.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |
| Installationspfad                                                                           | <p>Der Standardpfad ist C:\Programme\ NetApp\ SnapCenter. Optional können Sie den Pfad anpassen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Alle Hosts im Cluster hinzufügen                                                            | <p>Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einer WSFC- oder SQL-Verfügbarkeitsgruppe hinzuzufügen. Sie sollten alle Clusterknoten hinzufügen, indem Sie das entsprechende Cluster-Kontrollkästchen in der GUI aktivieren, wenn Sie mehrere verfügbare SQL-Verfügbarkeitsgruppen innerhalb eines Clusters verwalten und identifizieren möchten.</p>                                                                                                                                                                   |
| Vorinstallationsprüfungen überspringen                                                      | <p>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.</p>                                                                                                                                                                                                                                                                                                                                 |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | <p>Aktivieren Sie dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.</p> <p>Geben Sie den gMSA-Namen im folgenden Format an: Domänenname\Kontoname\$.</p> <div>  <p>Wenn der Host mit gMSA hinzugefügt wird und das gMSA über Anmelde- und Systemadministratorrechte verfügt, wird das gMSA zum Herstellen einer Verbindung mit der SQL-Instanz verwendet.</p> </div>        |



7. Wählen Sie **Senden**.

8. Wählen Sie für das SQL-Plug-in den Host aus, um das Protokollverzeichnis zu konfigurieren.

- a. Wählen Sie **Protokollverzeichnis konfigurieren** und wählen Sie auf der Seite „Host-Protokollverzeichnis konfigurieren“ die Option **Durchsuchen** aus und führen Sie die folgenden Schritte aus:

Zur Auswahl werden nur NetApp LUNs (Laufwerke) aufgelistet. SnapCenter sichert und repliziert das Host-Protokollverzeichnis als Teil des Sicherungsvorgangs.

Configure Plug-in for SQL Server

Configure the log backup directory for clusmigag.smsqlqa3.gdl.englab.netapp.com

Configure host log directory

Host

Host log directory

dedicated disk directory path

Apply Browse

Configure FCI instance log directory

FCI instance

Nothing selected

FCI log directory

shared disk directory path

Apply Browse

- i. Wählen Sie den Laufwerksbuchstaben oder Einhängepunkt auf dem Host aus, auf dem das Hostprotokoll gespeichert werden soll.
- ii. Wählen Sie bei Bedarf ein Unterverzeichnis.
- iii. Wählen Sie **Speichern**.

9. Wählen Sie **Senden**.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, 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, müssen Sie das Problem beheben.



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

10. Überwachen Sie den Installationsfortschritt.

### Installieren Sie das SnapCenter -Plug-in für Microsoft SQL Server mithilfe von Cmdlets auf mehreren Remotehosts

Sie können das SnapCenter Plug-in für Microsoft SQL Server mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

## Bevor Sie beginnen

Sie müssen sich auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

## Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das SnapCenter -Plug-in für Microsoft SQL Server auf mehreren Remote-Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

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"](#) .

Sie können die Option -skippercheck verwenden, 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.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

## Installieren Sie das SnapCenter -Plug-in für Microsoft SQL Server im Hintergrund über die Befehlszeile

Sie sollten das SnapCenter Plug-in für Microsoft SQL Server über die SnapCenter -Benutzeroberfläche installieren. Wenn dies aus irgendeinem Grund nicht möglich ist, können Sie das Installationsprogramm des Plug-ins für SQL Server unbeaufsichtigt im Hintergrundmodus über die Windows-Befehlszeile ausführen.

## Bevor Sie beginnen

- Sie müssen die frühere Version des SnapCenter -Plug-ins für Microsoft SQL Server vor der Installation löschen.

Weitere Informationen finden Sie unter ["So installieren Sie ein SnapCenter -Plug-In manuell und direkt vom Plug-In-Host"](#) .

## Schritte

1. Überprüfen Sie, ob der Ordner C:\temp auf dem Plug-In-Host vorhanden ist und der angemeldete Benutzer vollen Zugriff darauf hat.
2. Laden Sie das Plug-in für die SQL Server-Software von C:\ProgramData\NetApp\ SnapCenter\Package Repository herunter.

Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

3. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-In installieren möchten.
4. Navigieren Sie von einer Windows-Eingabeaufforderung auf dem lokalen Host zu dem Verzeichnis, in dem Sie die Plug-In-Installationsdateien gespeichert haben.
5. Installieren Sie das Plug-in für die SQL Server-Software:

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"  
/log"Log_Path" BI_SNAPCENTER_PORT=Num  
SUITE_INSTALLDIR="Install_Directory_Path"
```

```
BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCSQL
```

Ersetzen Sie die Platzhalterwerte durch Ihre Daten

- Debug\_Log\_Path ist der Name und der Speicherort der Protokolldatei des Suite-Installationsprogramms.
- Log\_Path ist der Speicherort der Installationsprotokolle der Plug-In-Komponenten (SCW, SCSQL und SMCore).
- Num ist der Port, über den SnapCenter mit SMCore kommuniziert
- Install\_Directory\_Path ist das Installationsverzeichnis des Host-Plug-In-Pakets.
- domain\administrator ist das SnapCenter -Plug-in für das Microsoft Windows-Webdienstkonto.
- „Passwort“ ist das Passwort für das SnapCenter -Plug-in für das Microsoft Windows-Webdienstkonto.  
"snapcenter\_windows\_host\_plugin.exe"/silent  
/debuglog"C:\HPPW\_SCSQL\_Install.log" /log"C:\\" BI\_SNAPCENTER\_PORT=8145  
SUITE\_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI\_SERVICEACCOUNT=domain\administrator BI\_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL



Bei allen während der Installation des Plug-ins für SQL Server übergebenen Parametern wird zwischen Groß- und Kleinschreibung unterschieden.

6. Überwachen Sie den Windows-Taskplaner, die Hauptinstallationsprotokolldatei C:\Installdebug.log und die zusätzlichen Installationsdateien in C:\Temp.
7. Überwachen Sie das Verzeichnis %temp%, um sicherzustellen, dass die Installationsprogramme von msix.exe die Software fehlerfrei installieren.



Bei der Installation des Plug-ins für SQL Server wird das Plug-in auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie können das Plug-In auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder des PowerShell-Cmdlets hinzufügen. Nachdem der Host hinzugefügt wurde, wird das Plug-In automatisch erkannt.

## Überwachen Sie den Status der Installation des Plug-ins für SQL Server

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

### CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

## Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.

2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

### Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

#### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:

- a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-Childitem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

### Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

#### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-In-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

### 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.

## Konfigurieren der Notfallwiederherstellung

### Notfallwiederherstellung des SnapCenter -Plug-ins für SQL Server

Wenn das SnapCenter -Plug-in für SQL Server ausgefallen ist, führen Sie die folgenden Schritte aus, um zu einem anderen SQL-Host zu wechseln und die Daten wiederherzustellen.

## Bevor Sie beginnen

- Der sekundäre Host sollte dasselbe Betriebssystem, dieselbe Anwendung und denselben Hostnamen wie der primäre Host haben.
- Übertragen Sie das SnapCenter -Plug-in für SQL Server mithilfe der Seite **Host hinzufügen** oder **Host ändern** auf einen alternativen Host. Sehen ["Hosts verwalten"](#) für weitere Informationen.

## Schritte

1. Wählen Sie den Host auf der Seite **Hosts** aus, um das SnapCenter -Plug-In für SQL Server zu ändern und zu installieren.
2. (Optional) Ersetzen Sie die Konfigurationsdateien des SnapCenter -Plug-ins für SQL Server aus der Notfallwiederherstellungssicherung (DR) auf dem neuen Computer.

3. Importieren Sie Windows- und SQL-Zeitpläne aus dem Ordner „SnapCenter Plug-in für SQL Server“ aus der DR-Sicherung.

### Ähnliche Informationen

Siehe die ["APIs zur Notfallwiederherstellung"](#) Video.

### Speicher-Notfallwiederherstellung (DR) für SnapCenter Plug-in für SQL Server

Sie können das SnapCenter Plug-in für SQL Server-Speicher wiederherstellen, indem Sie auf der Seite „Globale Einstellungen“ den DR-Modus für Speicher aktivieren.

#### Bevor Sie beginnen

- Stellen Sie sicher, dass sich die Plug-Ins im Wartungsmodus befinden.
- Brechen Sie die Beziehung zwischen SnapMirror und SnapVault ab. ["Aufbrechen von SnapMirror-Beziehungen"](#)
- Verbinden Sie die LUN vom sekundären Computer mit dem Hostcomputer mit demselben Laufwerksbuchstaben.
- Stellen Sie sicher, dass alle Festplatten mit denselben Laufwerksbuchstaben verbunden sind, die vor der Notfallwiederherstellung verwendet wurden.
- Starten Sie den MSSQL-Serverdienst neu.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

#### Informationen zu diesem Vorgang

Disaster Recovery (DR) wird bei VMDK- und RDM-Konfigurationen nicht unterstützt.

#### Schritte

1. Navigieren Sie auf der Seite „Einstellungen“ zu **Einstellungen > Globale Einstellungen > Notfallwiederherstellung**.
2. Wählen Sie **Notfallwiederherstellung aktivieren**.
3. Klicken Sie auf **Übernehmen**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Überwachen > Jobs** klicken.

#### Nach Abschluss

- Wenn nach dem Failover neue Datenbanken erstellt werden, befinden sich die Datenbanken im Nicht-DR-Modus.

Die neuen Datenbanken funktionieren weiterhin wie vor dem Failover.

- Die neuen Backups, die im DR-Modus erstellt wurden, werden auf der Seite „Topologie“ unter SnapMirror oder SnapVault (sekundär) aufgelistet.

Neben den neuen Sicherungen wird ein „i“-Symbol angezeigt, um anzuzeigen, dass diese Sicherungen im DR-Modus erstellt wurden.

- Sie können das SnapCenter -Plug-In für SQL Server-Sicherungen, die während des Failovers erstellt wurden, entweder über die Benutzeroberfläche oder das folgende Cmdlet löschen: `Remove-SmBackup`
- Wenn Sie möchten, dass sich einige der Ressourcen nach dem Failover im Nicht-DR-Modus befinden, verwenden Sie das folgende Cmdlet: `Remove-SmResourceDRMode`



Weitere Informationen finden Sie im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

- SnapCenter Server verwaltet die einzelnen Speicherressourcen (SQL-Datenbanken), die sich im DR- oder Nicht-DR-Modus befinden, jedoch nicht die Ressourcengruppe mit Speicherressourcen, die sich im DR-Modus oder Nicht-DR-Modus befinden.

### Failback vom SnapCenter Plug-in für den sekundären SQL Server-Speicher zum primären Speicher

Nachdem das SnapCenter -Plug-In für den primären SQL Server-Speicher wieder online ist, sollten Sie ein Failback auf den primären Speicher durchführen.

#### Bevor Sie beginnen

- Versetzen Sie das SnapCenter -Plug-in für SQL Server auf der Seite „Verwaltete Hosts“ in den Wartungsmodus.
- Trennen Sie den sekundären Speicher vom Host und stellen Sie eine Verbindung vom primären Speicher her.
- Um ein Failback zum primären Speicher durchzuführen, stellen Sie sicher, dass die Beziehungsrichtung dieselbe bleibt wie vor dem Failover, indem Sie den umgekehrten Resynchronisierungsvorgang durchführen.

Um die Rollen des primären und sekundären Speichers nach dem umgekehrten Resynchronisierungsvorgang beizubehalten, führen Sie den umgekehrten Resynchronisierungsvorgang noch einmal durch.

Weitere Informationen finden Sie unter ["Umgekehrte Neusynchronisierung von Spiegelbeziehungen"](#)

- Starten Sie den MSSQL-Serverdienst neu.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.



Während eines Failovers oder Failbacks des Plug-Ins wird der Gesamtstatus des Plug-Ins nicht sofort aktualisiert. Der Gesamtstatus des Hosts und des Plug-Ins wird während des nachfolgenden Host-Aktualisierungsvorgangs aktualisiert.

#### Schritte

1. Navigieren Sie auf der Seite „Einstellungen“ zu **Einstellungen > Globale Einstellungen > Notfallwiederherstellung**.
2. Deaktivieren Sie **Notfallwiederherstellung aktivieren**.
3. Klicken Sie auf **Übernehmen**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Überwachen > Jobs** klicken.

#### Nach Abschluss

Sie können das SnapCenter -Plug-In für SQL Server-Sicherungen, die während des Failovers erstellt wurden, entweder über die Benutzeroberfläche oder das folgende Cmdlet löschen: `Remove-SmDRFailoverBackups`

## 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 Datenschutz vor

### Voraussetzungen für die Verwendung des SnapCenter -Plug-ins für Microsoft SQL Server

Bevor Sie mit der Verwendung des Plug-ins für SQL Server beginnen, muss der SnapCenter Administrator SnapCenter Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich bei SnapCenter an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen oder zuweisen und Anmeldeinformationen erstellen.



SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss einen eindeutigen Namen haben.

- Fügen Sie Hosts hinzu, installieren Sie die Plug-Ins, ermitteln (aktualisieren) Sie die Ressourcen und konfigurieren Sie die Plug-Ins.
- Verschieben Sie eine vorhandene Microsoft SQL Server-Datenbank von einer lokalen Festplatte auf eine NetApp LUN oder umgekehrt, indem Sie `Invoke-SmConfigureResources` ausführen.

Informationen zum Ausführen des Cmdlets finden Sie im ["Referenzhandbuch für SnapCenter -Software -Cmdlets"](#)

- Wenn Sie SnapCenter Server zum Schutz von SQL-Datenbanken 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. Weitere Informationen finden Sie in der Dokumentation zum SnapCenter Plug-in for VMware vSphere .

["SnapCenter Plug-in for VMware vSphere Dokumentation"](#)

- Führen Sie die hostseitige Speicherbereitstellung mit dem SnapCenter -Plug-in für Microsoft Windows durch.

- Richten Sie SnapMirror und SnapVault -Beziehungen ein, wenn Sie eine Backup-Replikation wünschen.

Weitere Informationen finden Sie in den Installationsinformationen zu SnapCenter .

Für Benutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.1.1 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme. Für Benutzer von SnapCenter 4.2.x sowie NetApp Data Broker 1.0 und 1.0.1 enthält die Dokumentation Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des SnapCenter Plug-in for VMware vSphere, das von der Linux-basierten virtuellen NetApp Data Broker-Appliance (Open Virtual Appliance-Format) bereitgestellt wird. Für Benutzer von SnapCenter 4.3.x enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des Linux-basierten SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance-Format).

["SnapCenter Plug-in for VMware vSphere Dokumentation"](#)

## **So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SQL Server verwendet**

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei Ressourcen handelt es sich in der Regel um Datenbanken, Datenbankinstanzen oder Microsoft SQL Server-Verfügbarkeitsgruppen, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter -Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

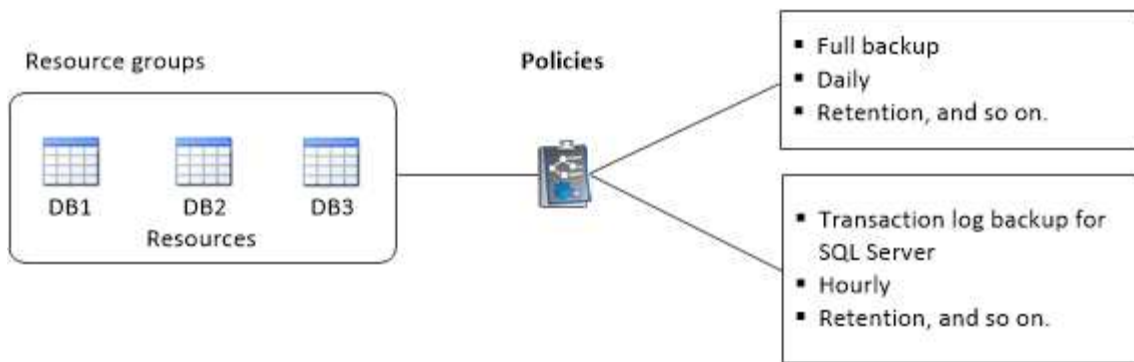
Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Sicherungshäufigkeit, die Aufbewahrung von Kopien, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

Stellen Sie sich eine Ressourcengruppe so vor, als würde sie definieren, *was* Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als würde sie definieren, *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme auf dem Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anfügen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird, und einen anderen Zeitplan, der stündlich Protokollsicherungen durchführt.

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



## Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe

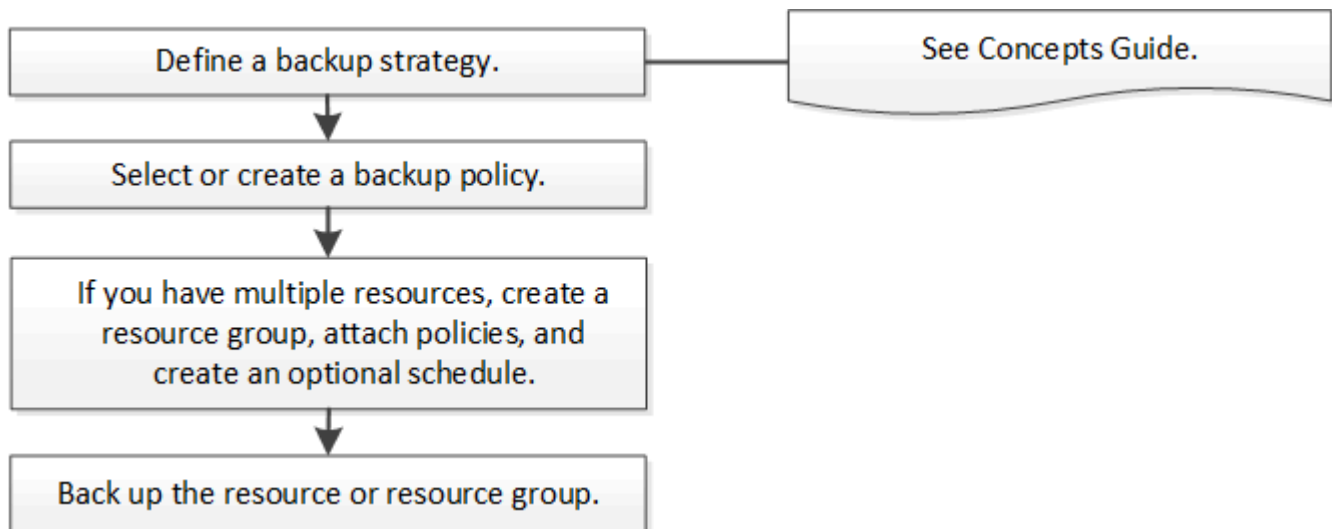
### Sicherungsworkflow

Wenn Sie das SnapCenter -Plug-in für Microsoft SQL Server in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern der SQL Server-Ressourcen verwenden.

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden.

Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Sicherungsvorgänge durchführen müssen:



Die Optionen „Jetzt sichern“, „Wiederherstellen“, „Sicherungen verwalten“ und „Klonen“ auf der Seite „Ressourcen“ sind deaktiviert, wenn Sie eine Nicht- NetApp -LUN, eine beschädigte Datenbank oder eine Datenbank auswählen, die wiederhergestellt wird.

Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs-, Überprüfungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#)

## So sichert SnapCenter Datenbanken

SnapCenter verwendet Snapshot-Technologie, um die SQL Server-Datenbanken zu sichern, die sich auf LUNs oder VMDKs befinden. SnapCenter erstellt das Backup, indem es Snapshots der Datenbanken erstellt.

Wenn Sie auf der Seite „Ressourcen“ eine Datenbank für eine vollständige Datenbanksicherung auswählen, wählt SnapCenter automatisch alle anderen Datenbanken aus, die sich auf demselben Speichervolume befinden. Wenn die LUN oder VMDK nur eine einzige Datenbank speichert, können Sie die Datenbank einzeln löschen oder erneut auswählen. Wenn die LUN oder VMDK mehrere Datenbanken enthält, müssen Sie die Datenbanken als Gruppe löschen oder erneut auswählen.

Alle Datenbanken, die sich auf einem einzelnen Volume befinden, werden gleichzeitig mithilfe von Snapshots gesichert. Wenn die maximale Anzahl gleichzeitiger Sicherungsdatenbanken 35 beträgt und sich mehr als 35 Datenbanken in einem Speichervolume befinden, entspricht die Gesamtzahl der erstellten Snapshots der Anzahl der Datenbanken geteilt durch 35.



Sie können die maximale Anzahl von Datenbanken für jeden Snapshot in der Sicherungsrichtlinie konfigurieren.

Wenn SnapCenter einen Snapshot erstellt, wird das gesamte Speichersystemvolume im Snapshot erfasst. Allerdings ist die Sicherung nur für den SQL-Hostserver gültig, für den die Sicherung erstellt wurde.

Wenn sich Daten von anderen SQL-Hostservern auf demselben Volume befinden, können diese Daten nicht aus dem Snapshot wiederhergestellt werden.

### Weitere Informationen finden

["Vorgänge zum Stilllegen oder Gruppieren von Ressourcen schlagen fehl"](#)

## Ermitteln, ob Ressourcen für die Sicherung verfügbar sind

Ressourcen sind die Datenbanken, Anwendungsinstanzen, Verfügbarkeitsgruppen und ähnliche Komponenten, die von den von Ihnen installierten Plug-Ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzaufgaben auszuführen. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Ihnen zur Verfügung stehen. Durch die Ermittlung der verfügbaren Ressourcen wird auch überprüft, ob die Plug-In-Installation erfolgreich abgeschlossen wurde.

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Um die Microsoft SQL-Datenbanken zu erkennen, muss eine der folgenden Bedingungen erfüllt sein.
  - Der Benutzer, der zum Hinzufügen des Plug-In-Hosts zum SnapCenter -Server verwendet wurde, sollte über die erforderlichen Berechtigungen (Sysadmin) auf dem Microsoft SQL-Server verfügen.
  - Wenn die obige Bedingung nicht erfüllt ist, sollten Sie im SnapCenter -Server den Benutzer konfigurieren, der über die erforderlichen Berechtigungen (Sysadmin) auf dem Microsoft SQL Server verfügt. Der Benutzer sollte auf der Ebene der Microsoft SQL Server-Instanz konfiguriert werden und kann ein SQL- oder Windows-Benutzer sein.

- Um die Microsoft SQL-Datenbanken in einem Windows-Cluster zu erkennen, müssen Sie den TCP/IP-Port der Failover Cluster Instance (FCI) entsperren.
- Wenn sich Datenbanken auf VMware RDM LUNs oder VMDKs 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"](#)

- Wenn der Host mit gMSA hinzugefügt wird und das gMSA über Anmelde- und Systemadministratorrechte verfügt, wird das gMSA zum Herstellen einer Verbindung mit der SQL-Instanz verwendet.

### Informationen zu diesem Vorgang

Sie können keine Datenbanken sichern, wenn die Option **Gesamtstatus** auf der Seite „Details“ auf „Nicht für Sicherung verfügbar“ eingestellt ist. Die Option **Gesamtstatus** wird auf „Nicht für Sicherung verfügbar“ gesetzt, wenn eine der folgenden Bedingungen zutrifft:

- Datenbanken befinden sich nicht auf einer NetApp LUN.
- Die Datenbanken befinden sich nicht im Normalzustand.

Datenbanken befinden sich nicht im Normalzustand, wenn sie offline sind, wiederhergestellt werden, die Wiederherstellung aussteht, verdächtig ist usw.

- Datenbanken verfügen über unzureichende Berechtigungen.

Wenn ein Benutzer beispielsweise nur Lesezugriff auf die Datenbank hat, können Dateien und Eigenschaften der Datenbank nicht identifiziert und daher nicht gesichert werden.



SnapCenter kann nur die primäre Datenbank sichern, wenn Sie über eine Verfügbarkeitsgruppenkonfiguration auf SQL Server Standard Edition verfügen.

### 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“ aus der Dropdown-Liste „Ansicht“ die Option „Datenbank“ oder „Instanz“ oder „Verfügbarkeitsgruppe“ aus.

Klicken  und wählen Sie den Hostnamen und die SQL Server-Instanz aus, um die Ressourcen zu filtern. Sie können dann auf , um den Filterbereich zu schließen.

3. Klicken Sie auf **Ressourcen aktualisieren**.

Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden im SnapCenter Server-Inventar aktualisiert.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Host- oder Clustername, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem Nicht-NetApp-Speicher befindet, Not available for backup wird in der Spalte **Gesamtstatus** angezeigt.

Sie können keine Datenschutzvorgänge für eine Datenbank durchführen, die sich auf einem Nicht NetApp -Speicher befindet.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, `Not protected` wird in der Spalte **Gesamtstatus** angezeigt.
- Wenn die Datenbank auf einem NetApp -Speichersystem liegt und geschützt ist, zeigt die Benutzeroberfläche `Backup not run` Meldung in der Spalte **Gesamtstatus**.
- Wenn die Datenbank auf einem NetApp Speichersystem liegt und geschützt ist und die Sicherung für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche `Backup succeeded` Meldung in der Spalte **Gesamtstatus**.



Wenn Sie beim Einrichten der Anmeldeinformationen eine SQL-Authentifizierung aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Vorhängeschlosssymbol angezeigt. Wenn das Vorhängeschlosssymbol angezeigt wird, müssen Sie die Anmeldeinformationen der Instanz oder Datenbank angeben, um die Instanz oder Datenbank erfolgreich zu einer Ressourcengruppe hinzuzufügen.

1. Nachdem der SnapCenter Administrator die Ressourcen einem RBAC-Benutzer zugewiesen hat, muss sich der RBAC-Benutzer anmelden und auf **Ressourcen aktualisieren** klicken, um den neuesten **Gesamtstatus** der Ressourcen anzuzeigen.

## Migrieren Sie Ressourcen zum NetApp Speichersystem

Nachdem Sie Ihr NetApp Speichersystem mit dem SnapCenter -Plug-in für Microsoft Windows bereitgestellt haben, können Sie Ihre Ressourcen entweder mithilfe der grafischen Benutzeroberfläche (GUI) von SnapCenter oder mithilfe der PowerShell-Cmdlets zum NetApp -Speichersystem oder von einer NetApp -LUN zu einer anderen NetApp -LUN migrieren.

### Bevor Sie beginnen

- Sie müssen dem SnapCenter Server Speichersysteme hinzugefügt haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. Die folgenden Informationen beschreiben einige der Felder, für die Sie möglicherweise Anleitungen benötigen.

### 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“ aus der Dropdown-Liste „Anzeigen“ die Option „Datenbank“ oder „Instanz“ aus.
3. Wählen Sie entweder die Datenbank oder die Instanz aus der Liste aus und klicken Sie auf **Migrieren**.
4. Führen Sie auf der Seite „Ressourcen“ die folgenden Aktionen aus:



| Für dieses Feld...                               | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Datenbankname</b> (optional)                  | Wenn Sie eine Instanz für die Migration ausgewählt haben, müssen Sie die Datenbanken dieser Instanz aus der Dropdown-Liste <b>Datenbanken</b> auswählen.                                                                                                                                                                       |
| <b>Ziele auswählen</b>                           | <p>Wählen Sie den Zielspeicherort für Daten- und Protokolldateien.</p> <p>Die Daten- und Protokolldateien werden in den Ordner „Daten“ bzw. „Protokoll“ unter dem ausgewählten NetApp Laufwerk verschoben. Wenn ein Ordner in der Ordnerstruktur nicht vorhanden ist, wird ein Ordner erstellt und die Ressource migriert.</p> |
| <b>Datenbankdateidetails anzeigen</b> (optional) | <p>Wählen Sie diese Option, wenn Sie mehrere Dateien einer einzelnen Datenbank migrieren möchten.</p> <div>  <p>Diese Option wird nicht angezeigt, wenn Sie die Ressource <b>Instanz</b> auswählen.</p> </div>                                |
| <b>Optionen</b>                                  | <p>Wählen Sie <b>Kopie der migrierten Datenbank am ursprünglichen Speicherort löschen</b>, um die Kopie der Datenbank aus der Quelle zu löschen.</p> <p>Optional: <b>FÜHREN SIE UPDATE STATISTICS für Tabellen aus, bevor Sie die Datenbank trennen.</b></p>                                                                   |

5. Führen Sie auf der Seite „Überprüfen“ die folgenden Aktionen aus:

| Für dieses Feld...                             | Machen Sie Folgendes...                                                                                                                                                                                    |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Optionen zur Datenbankkonsistenzprüfung</b> | Wählen Sie <b>Vorher ausführen</b> , um die Integrität der Datenbank vor der Migration zu überprüfen. Wählen Sie <b>Ausführen nach</b> , um die Integrität der Datenbank nach der Migration zu überprüfen. |



| Für dieses Feld...           | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DBCC CHECKDB-Optionen</b> | <ul style="list-style-type: none"> <li>Wählen Sie die Option <b>PHYSICAL_ONLY</b>, um die Integritätsprüfung auf die physische Struktur der Datenbank zu beschränken und beschädigte Seiten, Prüfsummenfehler und allgemeine Hardwarefehler zu erkennen, die sich auf die Datenbank auswirken.</li> <li>Wählen Sie die Option <b>NO_INFOMSGS</b>, um alle Informationsmeldungen zu unterdrücken.</li> <li>Wählen Sie die Option <b>ALL_ERRORMSGs</b>, um alle gemeldeten Fehler pro Objekt anzuzeigen.</li> <li>Wählen Sie die Option <b>NOINDEX</b>, wenn Sie nicht gruppierte Indizes nicht überprüfen möchten.</li> </ul> <p>Die SQL Server-Datenbank verwendet den Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.</p> <div style="display: flex; align-items: center;">  <div> <p>Sie können diese Option auswählen, um die Ausführungszeit zu verkürzen.</p> </div> </div> <ul style="list-style-type: none"> <li>Wählen Sie die Option <b>TABLOCK</b>, um die Prüfungen einzuschränken und Sperren zu erhalten, anstatt einen internen Datenbank-Snapshot zu verwenden.</li> </ul> |

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

## Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, bevor Sie SnapCenter zum Sichern von SQL Server-Ressourcen verwenden, oder Sie können eine Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine einzelne Ressource sichern.

### Bevor Sie beginnen

- Sie müssen Ihre Datenschutzstrategie definiert haben.
- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Sie müssen das Host-Protokollverzeichnis für die Protokollsicherung konfiguriert haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss der SnapCenter Administrator Ihnen

die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.

Informationen dazu, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den Installationsinformationen zu SnapCenter .

- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des Parameters usePowershellProcessforScripts in der Datei web.config auf true setzen.

Der Standardwert ist „false“.

- 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

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten und aufbewahren und wie häufig die Ressource oder Ressourcengruppe gesichert wird. Darüber hinaus können Sie Replikations- und Skripteinstellungen angeben. Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- 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.

### Schritt 1: Richtliniennamen erstellen

1. Wählen Sie im linken Navigationsbereich **Einstellungen** aus.
2. Wählen Sie auf der Seite „Einstellungen“ **Richtlinien** aus.
3. Wählen Sie **Neu**.
4. Geben Sie auf der Seite **Name** den Richtliniennamen und die Details ein.

## Schritt 2: Richtlinienoptionen konfigurieren

1. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie Ihren Speichertyp aus.
  - b. Wählen Sie Ihren Richtlinienumfang aus.

### Vollständige Sicherung und Protokollsicherung

Sichern Sie die Datenbankdateien und Transaktionsprotokolle und kürzen Sie die Transaktionsprotokolle.

- i. Wählen Sie **Vollständige Sicherung und Protokollsicherung**.
- ii. Geben Sie die maximale Anzahl der Datenbanken ein, die für jeden Snapshot gesichert werden sollen.



Sie müssen diesen Wert erhöhen, wenn Sie mehrere Sicherungsvorgänge gleichzeitig ausführen möchten.

### Vollständige Sicherung

Sichern Sie die Datenbankdateien.

- i. Wählen Sie **Vollständige Sicherung**.
- ii. Geben Sie die maximale Anzahl der Datenbanken ein, die für jeden Snapshot gesichert werden sollen. Der Standardwert ist 100



Sie müssen diesen Wert erhöhen, wenn Sie mehrere Sicherungsvorgänge gleichzeitig ausführen möchten.

### Protokollsicherung

- i. Sichern Sie die Transaktionsprotokolle.
- ii. Wählen Sie **Protokollsicherung**.

### Nur Kopie-Backup

- i. Wenn Sie Ihre Ressourcen mithilfe einer anderen Sicherungsanwendung sichern, wählen Sie **Nur Sicherung kopieren**.

Wenn die Transaktionsprotokolle intakt bleiben, kann jede Sicherungsanwendung die Datenbanken wiederherstellen. Normalerweise sollten Sie die Option „Nur kopieren“ unter keinen anderen Umständen verwenden.



Microsoft SQL unterstützt die Option **Nur Kopie-Sicherung** zusammen mit der Option **Vollständige Sicherung und Protokollsicherung** für sekundären Speicher nicht.

## Schritt 3: Konfigurieren der Verfügbarkeitsgruppeneinstellungen

1. Führen Sie im Abschnitt „Einstellungen der Verfügbarkeitsgruppe“ die folgenden Aktionen aus:

- a. Sicherung nur auf bevorzugter Sicherungsreplik.

Wählen Sie diese Option, um nur auf der bevorzugten Sicherungsreplik zu sichern. Das bevorzugte Sicherungsreplik wird durch die für die AG im SQL Server konfigurierten Sicherungseinstellungen bestimmt.

- b. Wählen Sie Replikate für die Sicherung aus.

Wählen Sie für die Sicherung das primäre AG-Replikat oder das sekundäre AG-Replikat aus.

- c. Wählen Sie die Sicherungspriorität (minimale und maximale Sicherungspriorität)

Geben Sie eine minimale und eine maximale Sicherungsprioritätszahl an, die das AG-Replikat für die Sicherung bestimmen. Sie können beispielsweise eine Mindestpriorität von 10 und eine Höchstpriorität von 50 festlegen. In diesem Fall werden alle AG-Replikate mit einer Priorität über 10 und unter 50 für die Sicherung berücksichtigt.

Standardmäßig beträgt die Mindestpriorität 1 und die Höchstpriorität 100.



In Clusterkonfigurationen werden die Sicherungen gemäß den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Knoten des Clusters aufbewahrt. Wenn sich der Besitzerknoten der AG ändert, werden die Sicherungen gemäß den Aufbewahrungseinstellungen erstellt und die Sicherungen des vorherigen Besitzerknotens bleiben erhalten. Die Aufbewahrung für AG gilt nur auf Knotenebene.

#### Schritt 4: Konfigurieren der Snapshot- und Replikationseinstellungen

1. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:

- a. Geben Sie den Zeitplantyp an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.

Sie können für eine Richtlinie nur einen Zeitplantyp auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungspläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

#### Schritt 5: Konfigurieren Sie aktuelle Aufbewahrungseinstellungen

1. Führen Sie im Abschnitt „Aktuelle Aufbewahrungseinstellungen“ je nach dem auf der Seite „Sicherungstyp“ ausgewählten Sicherungstyp eine oder mehrere der folgenden Aktionen aus:

### Spezifische Anzahl von Kopien

Behalten Sie nur eine bestimmte Anzahl von Snapshots.

1. Wählen Sie die Option **Protokollsicherungen der letzten <Anzahl> Tage aufbewahren** und geben Sie die Anzahl der Tage an, die aufbewahrt werden sollen. Wenn Sie sich diesem Limit nähern, möchten Sie möglicherweise ältere Kopien löschen.

### Bestimmte Anzahl von Tagen

Bewahren Sie die Sicherungskopien für eine bestimmte Anzahl von Tagen auf.

1. Wählen Sie die Option **Protokollsicherungen der letzten <Anzahl> Tage vollständiger Sicherungen aufbewahren** und geben Sie die Anzahl der Tage an, die die Protokollsicherungskopien aufbewahrt werden sollen.

## Schritt 6: Snapshot-Einstellungen konfigurieren

1. Führen Sie für die Aufbewahrungseinstellungen für vollständige Sicherungen die folgenden Aktionen aus:

- a. Geben Sie die Gesamtzahl der aufzubewahrenden Snapshots an
  - i. Um die Anzahl der aufzubewahrenden Snapshots anzugeben, wählen Sie **Aufzubewahrende Kopien**.
  - ii. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.



Standardmäßig ist der Wert für die Aufbewahrungsanzahl auf 2 eingestellt. 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.



Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden NetApp ONTAP Version unterstützt wird.

2. Aufbewahrungsdauer von Snapshots

- a. Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden, wählen Sie **Kopien aufbewahren für**.

3. 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.

4. Wählen Sie eine 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.

## Schritt 7: Konfigurieren sekundärer Replikationsoptionen

1. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

### SnapMirror aktualisieren

Aktualisieren Sie SnapMirror, nachdem Sie eine lokale Snapshot-Kopie erstellt haben.

1. Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) zu erstellen.

Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.

Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.

Sehen ["Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“"](#) .

### SnapVault aktualisieren

Aktualisieren Sie SnapVault , nachdem Sie eine Snapshot-Kopie erstellt haben.

1. Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen.

Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.

Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.

Weitere Informationen zu SnapLock Vault finden Sie unter ["Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel"](#)

Sehen ["Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“"](#) .

### Fehlerwiederholungsanzahl

1. Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird.

## Schritt 8: Skripteinstellungen konfigurieren

1. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Sicherungsvorgang ausgeführt werden soll.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren und Protokolle zu senden.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.



Sie müssen die SnapMirror Aufbewahrungsrichtlinie in ONTAP so konfigurieren, dass der sekundäre Speicher die maximale Anzahl an Snapshots nicht erreicht.

## Schritt 9: Konfigurieren der Überprüfungseinstellungen

Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

1. Wählen Sie im Abschnitt „Überprüfung für folgende Sicherungszeitpläne ausführen“ die Zeitplanhäufigkeit aus.
2. Führen Sie im Abschnitt „Optionen zur Datenbankkonsistenzprüfung“ die folgenden Aktionen aus:
  - a. Beschränken Sie die Integritätsstruktur auf die physische Struktur der Datenbank (PHYSICAL\_ONLY).
    - i. Wählen Sie **Integritätsstruktur auf die physische Struktur der Datenbank beschränken (NUR\_PHYSIKALISCH)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu beschränken und zerrissene Seiten, Prüfsummenfehler und allgemeine Hardwarefehler zu erkennen, die sich auf die Datenbank auswirken.
  - b. Alle Informationsmeldungen unterdrücken (NO\_INFOMSGS)
    - i. Wählen Sie **Alle Informationsmeldungen unterdrücken (NO\_INFOMSGS)**, um alle Informationsmeldungen zu unterdrücken. Standardmäßig ausgewählt.
  - c. Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL\_ERRORMSGs)
    - i. Wählen Sie **Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL\_ERRORMSGs)**, um alle gemeldeten Fehler pro Objekt anzuzeigen.
  - d. Nicht gruppierte Indizes nicht prüfen (NOINDEX)
    - i. Wählen Sie **Nicht gruppierte Indizes nicht prüfen (NOINDEX)** aus, wenn Sie keine nicht gruppierten Indizes prüfen möchten. Die SQL Server-Datenbank verwendet den Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.
  - e. Begrenzen Sie die Prüfungen und erhalten Sie die Sperren, anstatt einen internen Datenbank-Snapshot (TABLOCK) zu verwenden.
    - i. Wählen Sie **Beschränken Sie die Prüfungen und erhalten Sie die Sperren, anstatt eine interne Datenbank-Snapshot-Kopie zu verwenden (TABLOCK)** aus, um die Prüfungen zu begrenzen und Sperren zu erhalten, anstatt einen internen Datenbank-Snapshot zu verwenden.
3. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss überprüfen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
4. Geben Sie im Abschnitt **Einstellungen des Überprüfungsskripts** den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Überprüfungsvorgang ausgeführt werden soll.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

## Schritt 10: Zusammenfassung der Überprüfung

1. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

## Erstellen von Ressourcengruppen und Anfügen von Richtlinien für SQL Server

Eine Ressourcengruppe ist ein Container, zu dem Sie Ressourcen hinzufügen, die Sie

gemeinsam sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die einer bestimmten Anwendung zugeordnet sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

Sie können Ressourcen einzeln schützen, ohne eine neue Ressourcengruppe zu erstellen. Sie können Backups der geschützten Ressource erstellen.

Informationen zu diesem Vorgang

- 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.
- Das Hinzufügen neuer Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken 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. 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 „Datenbank“ aus.



Wenn Sie SnapCenter kürzlich eine Ressource hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie auf **Neue Ressourcengruppe**.
4. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name               | <div>Geben Sie den Namen der Ressourcengruppe ein.</div> <div> Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</div>                                                                                                                               |
| Schlagwörter       | Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden. |



| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                  |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel:<br>customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt. |

5. Führen Sie auf der Seite „Ressourcen“ die folgenden Schritte aus:

- a. Wählen Sie den Hostnamen, den Ressourcentyp und die SQL Server-Instanz aus den Dropdown-Listen aus, um die Liste der Ressourcen zu filtern.



Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

- b. Um Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben, führen Sie einen der folgenden Schritte aus:

- Wählen Sie **Alle Ressourcen auf demselben Speichervolume automatisch auswählen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
- Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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

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

- b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **OK**.

Sie müssen dies für jede in der Richtlinie aufgeführte Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

- d. Wählen Sie den Microsoft SQL Server-Scheduler aus.

Sie müssen außerdem eine Scheduler-Instanz auswählen, die mit der Planungsrichtlinie verknüpft werden soll.

Wenn Sie den Microsoft SQL Server-Scheduler nicht auswählen, wird standardmäßig der Microsoft Windows-Scheduler verwendet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden. Sie sollten die Zeitpläne nicht ändern und den im Windows-Scheduler oder SQL Server-Agent erstellten Sicherungsauftrag nicht umbenennen.

7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

- a. Wählen Sie den Verifizierungsserver aus der Dropdown-Liste **Verifizierungsserver** aus.

Die Liste enthält alle in SnapCenter hinzugefügten SQL-Server. Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).



Die Version des Überprüfungsservers sollte mit der Version und Edition des SQL-Servers übereinstimmen, auf dem die primäre Datenbank gehostet wird.

- a. Klicken Sie auf **Locators laden**, um die SnapMirror und SnapVault -Volumes zu laden und die Überprüfung auf dem sekundären Speicher durchzuführen.
- b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf \*  \*.
- 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 <b>Überprüfung nach Sicherung ausführen</b> . |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> .       |

- d. Klicken Sie auf **OK**.

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

Überprüfung und anschließend die Bearbeitung durchführen, indem Sie auf \* klicken.  \* oder durch Klicken auf \* löschen  \*.

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-SmSmtServer“ angegeben haben.

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

## Ähnliche Informationen

["Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken"](#)

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Microsoft SQL Server-Ressourcen 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                                                                         |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> .                                                        |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Voraussetzungen für die Sicherung von SQL-Ressourcen

Bevor Sie eine SQL-Ressource sichern, müssen Sie sicherstellen, dass mehrere Anforderungen erfüllt sind.

- Sie müssen eine Ressource von einem Nicht- NetApp -Speichersystem auf ein NetApp -Speichersystem migriert haben.
- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror -Beziehung zu einem sekundären Speicher sichern möchten, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Der von einem Active Directory (AD)-Benutzer initiierte Sicherungsvorgang schlägt fehl, wenn die Anmeldeinformationen der SQL-Instanz nicht dem AD-Benutzer oder der AD-Gruppe zugewiesen sind. Sie müssen die Anmeldeinformationen der SQL-Instanz dem AD-Benutzer oder der AD-Gruppe auf der Seite

**Einstellungen > Benutzerzugriff** zuweisen.

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet ausgelöst wird. Sie sollten den Wert von `FMaxRetryForUninitializedHosts` in `web.config` mithilfe des PS-Cmdlets `Set-SmConfigSettings` konfigurieren.

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Ausführen von Datenschutzvorgängen verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Verwaltungs-LIF-IP-Adresse haben.

### Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets `Open-SmConnection`.

Dieses Beispiel öffnet eine PowerShell-Sitzung:

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

In diesem Beispiel wird eine neue Anmeldeinformation mit dem Namen „FinanceAdmin“ mit Windows-

Anmeldeinformationen erstellt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

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"](#) .

## Sichern von SQL-Ressourcen

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Informationen zu diesem Vorgang

- Um den Sicherungsvorgang zu optimieren, sollten Sie einen Reverse-Lookup-Datensatz der Windows-Clusternamen und IP-Adressen im DNS-Server erstellen.
- Für die Authentifizierung mit Windows-Anmeldeinformationen müssen Sie Ihre Anmeldeinformationen einrichten, bevor Sie die Plug-Ins installieren.
- Für die Authentifizierung der SQL Server-Instanz müssen Sie die Anmeldeinformationen nach der Installation der Plug-Ins hinzufügen.
- Für die gMSA-Authentifizierung müssen Sie gMSA einrichten, während Sie den Host bei SnapCenter auf der Seite **Host hinzufügen** oder **Host ändern** registrieren, um gMSA zu aktivieren und zu verwenden.
- Wenn der Host mit gMSA hinzugefügt wird und das gMSA über Anmelde- und Systemadministratorrechte verfügt, darf das gMSA eine Verbindung zur SQL-Instanz herstellen.
  - SnapCenter überprüft, ob die Authentifizierung für SQL-Instanzen konfiguriert ist. Wenn die Authentifizierung konfiguriert ist, wird mit diesen Anmeldeinformationen auf die SQL-Instanz zugegriffen.
  - Wenn die Authentifizierung nicht konfiguriert ist, verwenden Sie gMSA, um zu prüfen, ob das SQL-Plug-In derzeit ausgeführt wird. Wenn das Plug-In aktiv ist, wird es verwendet, um eine Verbindung zur SQL-Instanz herzustellen.
  - Der Zugriff auf die SQL-Instanz erfolgt über die Windows-Anmeldeinformationsauthentifizierung, wenn weder die Authentifizierung für SQL-Instanzen konfiguriert ist noch das Plug-In betriebsbereit ist.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdown-Liste „Anzeigen“ die Option „Datenbank“ oder „Instanz“ oder „Verfügbarkeitsgruppe“ aus.

- a. Wählen Sie die Datenbank, Instanz oder Verfügbarkeitsgruppe aus, die Sie sichern möchten.

Wenn Sie eine Sicherungskopie einer Instanz erstellen, sind die Informationen zum letzten Sicherungsstatus oder der Zeitstempel dieser Instanz auf der Ressourcenseite nicht verfügbar.

In der Topologieansicht können Sie nicht unterscheiden, ob es sich bei dem Sicherungsstatus, dem Zeitstempel oder der Sicherung um eine Instanz oder eine Datenbank handelt.

3. Aktivieren Sie auf der Seite „Ressourcen“ das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie** und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispielsweise customtext\_policy\_hostname oder resource\_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Führen Sie auf der Seite „Richtlinien“ die folgenden Aufgaben aus:

- a. Wählen Sie im Abschnitt „Richtlinien“ eine oder mehrere Richtlinien aus der Dropdownliste aus.

Sie können eine Richtlinie erstellen, indem Sie \* auswählen.  \* um den Richtlinienassistenten zu starten.

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

- b. Wählen \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Im Fenster **Zeitpläne für Richtlinie hinzufügen** `policy_name` Dialogfeld, konfigurieren Sie den Zeitplan und wählen Sie dann **OK**.

Hier `policy_name` ist der Name der Richtlinie, die Sie ausgewählt haben.

Die konfigurierten Zeitpläne werden in der Spalte **Angewandte Zeitpläne** aufgelistet.

- a. Wählen Sie **Microsoft SQL Server-Scheduler verwenden** und wählen Sie dann aus der Dropdown-Liste **Scheduler-Instanz** die Scheduler-Instanz aus, die der Planungsrichtlinie zugeordnet ist.

5. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

- a. Wählen Sie den Verifizierungsserver aus der Dropdown-Liste **Verifizierungsserver** aus.

Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).





Die Version des Verifizierungsservers sollte gleich oder höher sein als die Version der Edition des SQL-Servers, auf dem die primäre Datenbank gehostet wird.

- a. Wählen Sie **Sekundäre Locatoren laden, um Backups auf dem sekundären Speichersystem zu überprüfen**, um Ihre Backups auf dem sekundären Speichersystem zu überprüfen.
- b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und wählen Sie dann \*  \*.
- c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen *Richtliniennamen*“ die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                  |
|------------------------------------------------------|----------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> . |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> .       |



Wenn der Überprüfungsserver keine Speicherverbindung hat, schlägt der Überprüfungsvorgang mit folgendem Fehler fehl: „Datenträger konnte nicht eingebunden werden.“

- d. Wählen Sie **OK**.

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

6. 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-SmSmtServer“ angegeben haben.

7. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Die Seite „Datenbanktopologie“ wird angezeigt.

8. Wählen Sie **Jetzt sichern**.

9. 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. Wählen Sie **Nach Sicherung überprüfen**, um Ihre Sicherung zu überprüfen.

c. Wählen Sie **Backup**.



Sie sollten den im Windows-Scheduler oder SQL Server-Agent erstellten Sicherungsauftrag nicht umbenennen.

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.

Es wird eine implizite Ressourcengruppe erstellt. Sie können dies anzeigen, indem Sie den entsprechenden Benutzer oder die entsprechende Gruppe auf der Seite „Benutzerzugriff“ auswählen. Der implizite Ressourcengruppentyp ist „Ressource“.

10. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen > Jobs** auswählen.

### Nach Abschluss

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl. Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`.

### Ähnliche Informationen

["Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken"](#)

["Sicherungsvorgänge schlagen aufgrund der Verzögerung im TCP\\_TIMEOUT mit einem MySQL-Verbindungsfehler fehl"](#)

["Die Sicherung schlägt mit einem Windows-Planerfehler fehl"](#)

["Vorgänge zum Stilllegen oder Gruppieren von Ressourcen schlagen fehl"](#)

### PowerShell-Cmdlets

#### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets `Add-SmPolicy`.

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem SQL-Sicherungstyp „FullBackup“ erstellt:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem Sicherungstyp „CrashConsistent“ für das Windows-Dateisystem erstellt:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

### 3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „Get-SmResources“.

Dieses Beispiel ermittelt die Ressourcen für das Microsoft SQL-Plug-In auf dem angegebenen Host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

Dieses Beispiel ermittelt die Ressourcen für Windows-Dateisysteme auf dem angegebenen Host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

### 4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

In diesem Beispiel wird eine neue SQL-Datenbank-Sicherungsressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

In diesem Beispiel wird eine neue Ressourcengruppe zur Sicherung des Windows-Dateisystems mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

In diesem Beispiel wird ein Job-Zusammenfassungsbericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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"](#) .

## Sichern von SQL Server-Ressourcengruppen

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie  und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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. Wählen Sie nach der Sicherung „Überprüfen“ aus, um die On-Demand-Sicherung zu überprüfen.

Die Option **Überprüfen** in der Richtlinie gilt nur für geplante Jobs.

- c. Wählen Sie **Backup**.

5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Ähnliche Informationen

["Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken"](#)

["Erstellen von Ressourcengruppen und Anfügen von Richtlinien für SQL Server"](#)

["Sicherungsvorgänge schlagen aufgrund der Verzögerung im TCP\\_TIMEOUT mit einem MySQL-Verbindungsfehler fehl"](#)

["Die Sicherung schlägt mit einem Windows-Planerfehler fehl"](#)

## Überwachen Sie Sicherungsvorgänge für SQL-Ressourcen auf der Seite „SnapCenter -Aufträge“.

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 für SQL-Ressourcen 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.

## Abbrechen des SnapCenter -Plug-ins für Microsoft SQL Server-Sicherungsvorgänge

Sie können Sicherungsvorgänge abbrechen, die ausgeführt werden, in der Warteschlange stehen oder nicht reagieren. Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter Server den Vorgang und entfernt alle Snapshots aus dem Speicher, wenn die erstellte Sicherung nicht beim SnapCenter -Server registriert ist. Wenn die Sicherung bereits beim SnapCenter Server registriert ist, wird der bereits erstellte Snapshot auch nach dem Auslösen des Abbruchs nicht zurückgesetzt.

### Bevor Sie beginnen

- Sie müssen als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.
- Sie können nur Protokoll- oder vollständige Sicherungsvorgänge abbrechen, die sich in der Warteschlange befinden oder ausgeführt werden.
- Sie können den Vorgang nicht mehr abbrechen, nachdem die Überprüfung begonnen hat.

Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Überprüfungsvorgang wird nicht durchgeführt.

- Sie können einen Sicherungsvorgang entweder auf der Seite „Überwachen“ oder im Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter -GUI können Sie PowerShell-Cmdlets verwenden, um Vorgänge abzubrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

## Schritte

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>1. Wählen Sie im linken Navigationsbereich <b>Monitor</b> &gt; <b>Jobs</b> aus.</li><li>2. Wählen Sie den Auftrag aus und wählen Sie <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                                       |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>1. Nachdem Sie den Sicherungsauftrag gestartet haben, wählen Sie  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>2. Wählen Sie den Vorgang aus.</li><li>3. Wählen Sie auf der Seite „Auftragsdetails“ die Option „Auftrag abbrechen“ aus.</li></ol> |

## Ergebnis

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt. Wenn der Vorgang, den Sie abgebrochen haben, im Status „Abbrechen“ oder „Ausführen“ nicht reagiert, sollten Sie den `Cancel-SmJob -JobID <int> -Force Cmdlet`, um den Sicherungsvorgang zwangsweise zu beenden.

## Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“

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

### Informationen zu diesem Vorgang

Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen 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 es sich bei der ausgewählten Ressource um eine geklonte Datenbank handelt, schützen Sie die geklonte Datenbank. Die Quelle des Klon wird auf der Seite „Topologie“ angezeigt. Klicken Sie auf **Details**, um das zum Klonen verwendete Backup anzuzeigen.

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.

Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der Backups und Klone an.

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 die Anwendungsressource auf 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-, Umbenennungs- und Löschvorgänge durchzuführen.



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

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

## Bereinigen der Anzahl sekundärer Sicherungen mithilfe von PowerShell-Cmdlets

Sie können das Cmdlet „Remove-SmBackup“ verwenden, um die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshot zu bereinigen. Sie können dieses Cmdlet verwenden, wenn die Gesamtzahl der in der Topologie „Kopien verwalten“ angezeigten Snapshots nicht mit der Snapshot-Aufbewahrungseinstellung des sekundären Speichers übereinstimmt.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

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. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Bereinigen Sie die Anzahl sekundärer Sicherungen mit dem Parameter -CleanupSecondaryBackups.

In diesem Beispiel wird die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshots bereinigt:

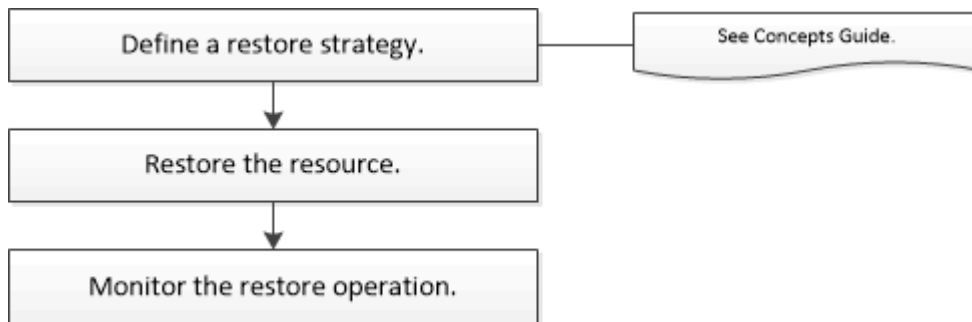
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

## Wiederherstellen von SQL Server-Ressourcen

### Wiederherstellungs-Workflow

Sie können SnapCenter zum Wiederherstellen von SQL Server-Datenbanken verwenden, indem Sie die Daten aus einer oder mehreren Sicherungen in Ihrem aktiven Dateisystem wiederherstellen und dann die Datenbank wiederherstellen. Sie können auch Datenbanken wiederherstellen, die sich in Verfügbarkeitsgruppen befinden, und die wiederhergestellten Datenbanken dann der Verfügbarkeitsgruppe hinzufügen. Bevor Sie eine SQL Server-Datenbank wiederherstellen, müssen Sie mehrere Vorbereitungsaufgaben durchführen.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Datenbankwiederherstellungsvorgänge durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs-, Überprüfungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#)

### Weitere Informationen finden

["Wiederherstellen einer SQL Server-Datenbank aus dem sekundären Speicher"](#)

["Wiederherstellen und Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets"](#)

["Der Wiederherstellungsvorgang schlägt unter Windows 2008 R2 möglicherweise fehl"](#)

### Voraussetzungen für die Wiederherstellung einer Datenbank

Bevor Sie eine SQL Server-Datenbank aus einem SnapCenter -Plug-in für Microsoft SQL Server-Backup wiederherstellen, müssen Sie sicherstellen, dass mehrere Anforderungen

erfüllt sind.

- Die SQL Server-Zielinstanz muss online und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.

Dies gilt sowohl für die Wiederherstellung von Benutzerdatenbanken als auch für die Wiederherstellung von Systemdatenbanken.

- SnapCenter -Vorgänge, die für die Ausführung mit den wiederherzustellenden SQL Server-Daten geplant sind, müssen deaktiviert werden. Dies gilt auch für alle auf Remoteverwaltungs- oder Remoteüberprüfungsservern geplanten Jobs.
- Wenn Systemdatenbanken nicht funktionsfähig sind, müssen Sie die Systemdatenbanken zunächst mit einem SQL Server-Dienstprogramm neu erstellen.
- Wenn Sie das Plug-In installieren, stellen Sie sicher, dass Sie anderen Rollen Berechtigungen zum Wiederherstellen der Sicherungen der Verfügbarkeitsgruppe (AG) erteilen.

Das Wiederherstellen der AG schlägt fehl, wenn eine der folgenden Bedingungen erfüllt ist:

- Wenn das Plug-In von einem RBAC-Benutzer installiert wird und ein Administrator versucht, eine AG-Sicherung wiederherzustellen
- Wenn das Plug-In von einem Administrator installiert wird und ein RBAC-Benutzer versucht, eine AG-Sicherung wiederherzustellen
- Wenn Sie benutzerdefinierte Protokollverzeichnissicherungen auf einem alternativen Host wiederherstellen, muss auf dem SnapCenter Server und dem Plug-In-Host dieselbe SnapCenter Version installiert sein.
- Sie müssen den Microsoft-Hotfix KB2887595 installiert haben. Weitere Informationen zu KB2887595 finden Sie auf der Microsoft-Support-Site.

["Microsoft-Supportartikel 2887595: Updaterollup für Windows RT 8.1, Windows 8.1 und Windows Server 2012 R2: November 2013"](#)

- Sie müssen die Ressourcengruppen oder die Datenbank gesichert haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.

Informationen dazu, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den Installationsinformationen zu SnapCenter .

- Alle Sicherungs- und Klonjobs müssen vor der Wiederherstellung der Datenbank gestoppt werden.
- Bei der Wiederherstellung kann es zu einer Zeitüberschreitung kommen, wenn die Datenbankgröße im Terabyte-Bereich (TB) liegt.

Sie müssen den Wert des RESTTimeout-Parameters von SnapCenter Server auf 20000000 ms erhöhen, indem Sie den folgenden Befehl ausführen: `Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}`. Je nach Größe der Datenbank kann der Timeout-Wert geändert werden. Der maximal einstellbare Wert beträgt 86400000 ms.

Wenn Sie die Datenbanken wiederherstellen möchten, während sie online sind, muss die Option „Online-Wiederherstellung“ auf der Seite „Wiederherstellen“ aktiviert sein.

## Wiederherstellen von SQL Server-Datenbanksicherungen

Sie können SnapCenter verwenden, um gesicherte SQL Server-Datenbanken wiederherzustellen. Die Datenbankwiederherstellung ist ein mehrphasiger Prozess, bei dem alle Daten und Protokollseiten aus einer angegebenen SQL Server-Sicherung in eine angegebene Datenbank kopiert werden.

### Informationen zu diesem Vorgang

- Sie können die gesicherten SQL Server-Datenbanken auf einer anderen SQL Server-Instanz auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde.

Sie können SnapCenter verwenden, um die gesicherten SQL Server-Datenbanken auf einem alternativen Pfad wiederherzustellen, sodass Sie keine Produktionsversion ersetzen.

- SnapCenter kann Datenbanken in einem Windows-Cluster wiederherstellen, ohne die SQL Server-Clustergruppe offline zu nehmen.
- Wenn während eines Wiederherstellungsvorgangs ein Clusterfehler (ein Clustergruppenverschiebungsvorgang) auftritt (z. B. wenn der Knoten, dem die Ressourcen gehören, ausfällt), müssen Sie die Verbindung zur SQL Server-Instanz wiederherstellen und den Wiederherstellungsvorgang anschließend neu starten.
- Sie können die Datenbank nicht wiederherstellen, wenn die Benutzer oder die SQL Server-Agent-Jobs auf die Datenbank zugreifen.
- Sie können Systemdatenbanken nicht auf einem alternativen Pfad wiederherstellen.
- Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- Die meisten Felder auf den Seiten des Wiederherstellungsassistenten sind selbsterklärend. Die folgenden Informationen beschreiben Felder, für die Sie möglicherweise Anleitungen benötigen.
- Für den Wiederherstellungsvorgang mit SnapMirror Active Sync müssen Sie die Sicherung vom primären Speicherort auswählen.
- 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.

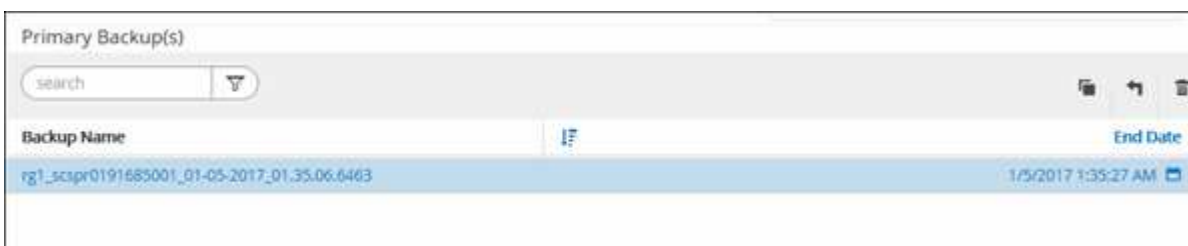
## SnapCenter -Benutzeroberfläche

### 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.

Die Topologieseite wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus dem Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf das  Symbol.



6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:

| Option                                                                                         | Beschreibung                                                                                                                                |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Stellen Sie die Datenbank auf demselben Host wieder her, auf dem die Sicherung erstellt wurde. | Wählen Sie diese Option, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Sicherungen erstellt wurden. |

| Option                                                               | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wiederherstellen der Datenbank auf einem alternativen Host           | <p>Wählen Sie diese Option, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem die Sicherungen durchgeführt werden.</p> <p>Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen an (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an.</p> <div>  <p>Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateierweiterung der ursprünglichen Datenbankdatei übereinstimmen.</p> </div> <p>Wenn die Option <b>Datenbank auf einem alternativen Host wiederherstellen</b> auf der Seite „Wiederherstellungsbereich“ nicht angezeigt wird, leeren Sie den Browser-Cache.</p> |
| Wiederherstellen der Datenbank mithilfe vorhandener Datenbankdateien | <p>Wählen Sie diese Option, wenn die Datenbank auf einem anderen SQL Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem die Sicherungen durchgeführt werden.</p> <p>Datenbankdateien sollten bereits in den angegebenen vorhandenen Dateipfaden vorhanden sein. Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen an (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an.</p>                                                                                                                                                                                                                                                                                                                                   |

7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:

| Option                    | Beschreibung                                                                                                                                                                           |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Keine                     | Wählen Sie <b>Keine</b> , wenn Sie nur die vollständige Sicherung ohne Protokolle wiederherstellen müssen.                                                                             |
| Alle Protokollsicherungen | Wählen Sie den minutengenauen Wiederherstellungsvorgang „Alle Protokollsicherungen“ aus, um alle verfügbaren Protokollsicherungen nach der vollständigen Sicherung wiederherzustellen. |

| Option                                             | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Durch Log-Backups bis                              | Wählen Sie <b>Nach Protokollsicherungen</b> aus, um einen Wiederherstellungsvorgang zu einem bestimmten Zeitpunkt durchzuführen, bei dem die Datenbank basierend auf Sicherungsprotokollen bis zum Sicherungsprotokoll mit dem ausgewählten Datum wiederhergestellt wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Nach einem bestimmten Datum bis                    | <p>Wählen Sie <b>Bis zu einem bestimmten Datum bis</b> aus, um das Datum und die Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht mehr auf die wiederhergestellte Datenbank angewendet werden.</p> <p>Dieser zeitpunktbezogene Wiederherstellungsvorgang stoppt die Wiederherstellung von Transaktionsprotokolleinträgen, die nach dem angegebenen Datum und der angegebenen Uhrzeit aufgezeichnet wurden.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Benutzerdefiniertes Protokollverzeichnis verwenden | <p>Wenn Sie <b>Alle Protokollsicherungen</b>, <b>Nach Protokollsicherungen</b> oder <b>Nach bestimmtem Datum bis</b> ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie <b>Benutzerdefiniertes Protokollverzeichnis verwenden</b> und geben Sie dann den Protokollspeicherort an.</p> <p>Die Option <b>Benutzerdefiniertes Protokollverzeichnis verwenden</b> ist nur verfügbar, wenn Sie <b>Datenbank auf einem anderen Host wiederherstellen</b> oder <b>Datenbank mit vorhandenen Datenbankdateien wiederherstellen</b> ausgewählt haben. Sie können auch den freigegebenen Pfad verwenden, stellen Sie jedoch sicher, dass der Pfad für den SQL-Benutzer zugänglich ist.</p> <div>  <p>Das benutzerdefinierte Protokollverzeichnis wird für die Verfügbarkeitsgruppendatenbank nicht unterstützt.</p> </div> |

8. Führen Sie auf der Seite „Pre Ops“ die folgenden Schritte aus:

- a. Wählen Sie auf der Seite „Optionen vor der Wiederherstellung“ eine der folgenden Optionen aus:
  - Wählen Sie **Datenbank beim Wiederherstellen mit gleichem Namen überschreiben**, um die Datenbank mit gleichem Namen wiederherzustellen.

- Wählen Sie **Replikationseinstellungen der SQL-Datenbank beibehalten**, um die Datenbank wiederherzustellen und die vorhandenen Replikationseinstellungen beizubehalten.
  - Wählen Sie **Transaktionsprotokollsicherung vor Wiederherstellung erstellen** aus, um vor Beginn des Wiederherstellungsvorgangs ein Transaktionsprotokoll zu erstellen.
  - Wählen Sie **Wiederherstellung beenden, wenn die Sicherung des Transaktionsprotokolls vor der Wiederherstellung fehlschlägt** aus, um den Wiederherstellungsvorgang abubrechen, wenn die Sicherung des Transaktionsprotokolls fehlschlägt.
- b. Geben Sie optionale Skripts an, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

9. Führen Sie auf der Seite „Post Ops“ die folgenden Schritte aus:

- a. Wählen Sie im Abschnitt „Datenbankstatus nach Abschluss der Wiederherstellung auswählen“ eine der folgenden Optionen aus:

- Wählen Sie **Betriebsbereit, aber nicht verfügbar zum Wiederherstellen zusätzlicher Transaktionsprotokolle**, wenn Sie jetzt alle erforderlichen Sicherungen wiederherstellen.

Dies ist das Standardverhalten, das die Datenbank durch Zurücksetzen der nicht festgeschriebenen Transaktionen einsatzbereit macht. Sie können keine weiteren Transaktionsprotokolle wiederherstellen, bis Sie eine Sicherung erstellt haben.

- Wählen Sie **Nicht betriebsbereit, aber zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar** aus, um die Datenbank nicht betriebsbereit zu lassen, ohne die nicht festgeschriebenen Transaktionen zurückzusetzen.

Zusätzliche Transaktionsprotokolle können wiederhergestellt werden. Sie können die Datenbank erst verwenden, wenn sie wiederhergestellt ist.

- Wählen Sie **Schreibgeschützter Modus, verfügbar zum Wiederherstellen zusätzlicher Transaktionsprotokolle**, um die Datenbank im schreibgeschützten Modus zu belassen.

Diese Option macht nicht festgeschriebene Transaktionen rückgängig, speichert die rückgängig gemachten Aktionen jedoch in einer Standby-Datei, sodass Wiederherstellungseffekte rückgängig gemacht werden können.

Wenn die Option „Verzeichnis rückgängig machen“ aktiviert ist, werden mehr Transaktionsprotokolle wiederhergestellt. Wenn der Wiederherstellungsvorgang für das Transaktionsprotokoll nicht erfolgreich ist, können die Änderungen rückgängig gemacht werden. Weitere Informationen finden Sie in der SQL Server-Dokumentation.

- b. Geben Sie optionale Skripts an, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.





Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

10. 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.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
12. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime | BackupType |
|----------|-------------------------------|------------|------------|
| -----    | -----                         | -----      | -----      |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:02:32   |
| AM       | Full Backup                   |            |            |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:23:17   |
| AM       |                               |            |            |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets `Restore-SmBackup` wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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"](#) .

## Wiederherstellen einer SQL Server-Datenbank aus dem sekundären Speicher

Sie können die gesicherten SQL Server-Datenbanken von den physischen LUNs (RDM, iSCSI oder FCP) auf einem sekundären Speichersystem wiederherstellen. Die Wiederherstellungsfunktion ist ein mehrphasiger Prozess, der alle Daten und Protokollseiten aus einer angegebenen SQL Server-Sicherung auf dem sekundären Speichersystem in eine angegebene Datenbank kopiert.

### Bevor Sie beginnen

- Sie müssen die Snapshots vom primären auf das sekundäre Speichersystem repliziert haben.
- Sie müssen sicherstellen, dass der SnapCenter Server und der Plug-In-Host eine Verbindung zum

sekundären Speichersystem herstellen können.

- Die meisten Felder auf den Seiten des Wiederherstellungsassistenten werden im grundlegenden Wiederherstellungsprozess erklärt. Die folgenden Informationen beschreiben einige der Felder, für die Sie möglicherweise Anleitungen benötigen.

### Informationen zu diesem Vorgang

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.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann \* SnapCenter Plug-in für SQL Server\* aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdownliste „Anzeigen“ die Option „Datenbank“ oder „Ressourcengruppe“ aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.

Die Seite mit der Datenbank- oder Ressourcengruppentopologie wird angezeigt.

4. Wählen Sie im Abschnitt „Kopien verwalten“ **Backups** aus dem sekundären Speichersystem (gespiegelt oder Tresor) aus.
5. Wählen Sie das Backup aus der Liste aus und klicken Sie dann auf .
6. Wählen Sie auf der Seite „Speicherort“ das Zielvolume für die Wiederherstellung der ausgewählten Ressource aus.
7. Schließen Sie den Wiederherstellungsassistenten ab, überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Wenn Sie eine Datenbank in einem anderen Pfad wiederhergestellt haben, der von anderen Datenbanken gemeinsam genutzt wird, sollten Sie eine vollständige Sicherung und Sicherungsüberprüfung durchführen, um sicherzustellen, dass Ihre wiederhergestellte Datenbank keine Beschädigungen auf physischer Ebene aufweist.

## Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets

Das Wiederherstellen einer Ressourcensicherung umfasst das Einleiten einer Verbindungssitzung mit dem SnapCenter -Server, das Auflisten der Sicherungen und Abrufen von Sicherungsinformationen sowie das Wiederherstellen einer Sicherung.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die

Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId    | BackupName                             | BackupTime  |
|-------------|----------------------------------------|-------------|
| BackupType  |                                        |             |
| -----       | -----                                  | -----       |
| 1           | Payroll Dataset_vise-f6_08... 8/4/2015 | 11:02:32 AM |
| Full Backup |                                        |             |
| 2           | Payroll Dataset_vise-f6_08... 8/4/2015 | 11:23:17 AM |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable        : False
IsRestartable        : False
IsCompleted          : False
IsVisible            : True
IsScheduled          : False
PercentageCompleted : 0
Description          :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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"](#).

## Reseed Availability Group-Datenbanken

Reseed ist eine Option zum Wiederherstellen von Datenbanken der Verfügbarkeitsgruppe (AG). Wenn die Synchronisierung einer sekundären Datenbank mit der primären Datenbank in einer AG aufgehoben wird, können Sie ein erneutes Seeding der sekundären Datenbank durchführen.

### Bevor Sie beginnen

- Sie müssen eine Sicherungskopie der sekundären AG-Datenbank erstellt haben, die Sie wiederherstellen möchten.
- Auf dem SnapCenter -Server und dem Plug-In-Host muss dieselbe SnapCenter -Version installiert sein.

### Informationen zu diesem Vorgang

- Sie können keinen Reseed-Vorgang für primäre Datenbanken durchführen.
- Sie können keinen Reseed-Vorgang durchführen, wenn die Replikatdatenbank aus der Verfügbarkeitsgruppe entfernt wird. Wenn das Replikat entfernt wird, schlägt der Reseed-Vorgang fehl.
- Während Sie den Reseed-Vorgang für die SQL-Verfügbarkeitsgruppendatenbank ausführen, sollten Sie keine Protokollsicherungen für die Replikatdatenbanken dieser Verfügbarkeitsgruppendatenbank auslösen. Wenn Sie während des Reseed-Vorgangs Protokollsicherungen auslösen, schlägt der Reseed-Vorgang mit der Fehlermeldung „Die Spiegeldatenbank „database\_name“ verfügt nicht über genügend Transaktionsprotokolldaten, um die Protokollsicherungskette der Hauptdatenbank beizubehalten“ fehl.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann \* SnapCenter Plug-in für SQL Server\* aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Ansicht“ die Option „Datenbank“ aus.
3. Wählen Sie die sekundäre AG-Datenbank aus der Liste aus.
4. Klicken Sie auf **Neu säen**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

## Überwachen von Wiederherstellungsvorgängen für SQL-Ressourcen

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.

## Abbrechen von Wiederherstellungsvorgängen für SQL-Ressourcen

Sie können in der Warteschlange befindliche Wiederherstellungsaufträge abbrechen.

Sie sollten als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzuberechnen.

### Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Wiederherstellungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Wiederherstellungsvorgänge abzuberechnen.
- Die Schaltfläche **Auftrag abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"> <li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li> <li>2. Wählen Sie den Auftrag aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li> </ol>                                                                                                                                                                                        |
| Aktivitätsbereich | <ol style="list-style-type: none"> <li>1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li> <li>2. Wählen Sie den Vorgang aus.</li> <li>3. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li> </ol> |

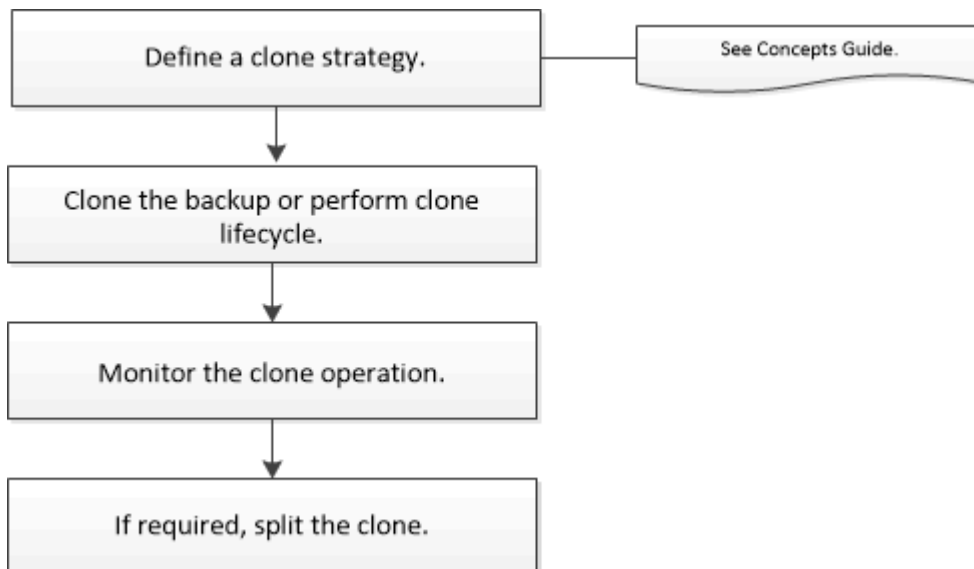
# Klonen von SQL Server-Datenbankressourcen

## Klon-Workflow

Sie müssen mit SnapCenter Server mehrere Aufgaben ausführen, bevor Sie Datenbankressourcen aus einer Sicherung klonen. Beim Datenbankklonen handelt es sich um den Vorgang, eine zeitpunktbezogene Kopie einer Produktionsdatenbank oder ihres Sicherungssatzes zu erstellen. Sie können Datenbanken klonen, um Funktionen zu testen, die während der Anwendungsentwicklungszyklen mit der aktuellen Datenbankstruktur und dem aktuellen Datenbankinhalt implementiert werden müssen, um beim Auffüllen von Data Warehouses die Tools zur Datenextraktion und -bearbeitung zu verwenden oder um Daten wiederherzustellen, die versehentlich gelöscht oder geändert wurden.

Ein Datenbankklonvorgang generiert Berichte basierend auf den Job-IDs.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Klonvorgänge durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs-, Überprüfungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#)

## Weitere Informationen finden

["Klonen aus einer SQL Server-Datenbanksicherung"](#)

["Klon-Lebenszyklus durchführen"](#)

["Der Klonvorgang kann mit dem Standardwert TCP\\_TIMEOUT fehlschlagen oder länger dauern"](#)

## Klonen aus einer SQL Server-Datenbanksicherung

Sie können SnapCenter verwenden, um eine SQL Server-Datenbanksicherung zu

klonen. Wenn Sie auf eine ältere Version der Daten zugreifen oder diese wiederherstellen möchten, können Sie Datenbanksicherungen bei Bedarf klonen.

### Bevor Sie beginnen

- Sie sollten sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Speichersystemverbindungen erledigt haben.
- Sie sollten Datenbanken oder Ressourcengruppen gesichert haben.
- Der Schutztyp, z. B. Spiegel, Tresor oder Spiegel-Tresor, für Daten-LUN und Protokoll-LUN sollte identisch sein, um beim Klonen auf einen alternativen Host mithilfe von Protokollsicherungen sekundäre Locatoren zu ermitteln.
- Wenn das gemountete Klonlaufwerk während eines SnapCenter -Klonvorgangs nicht gefunden werden kann, sollten Sie den CloneRetryTimeout-Parameter des SnapCenter Servers auf 300 ändern.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.

### Informationen zu diesem Vorgang

- Stellen Sie beim Klonen auf eine eigenständige Datenbankinstanz sicher, dass der Mount-Point-Pfad vorhanden ist und es sich um eine dedizierte Festplatte handelt.
- Stellen Sie beim Klonen auf eine Failoverclusterinstanz (FCI) sicher, dass die Bereitstellungspunkte vorhanden sind, es sich um eine gemeinsam genutzte Festplatte handelt und der Pfad und die FCI zur selben SQL-Ressourcengruppe gehören.
- Stellen Sie sicher, dass an jeden Host nur ein vFC- oder FC-Initiator angeschlossen ist. Dies liegt daran, dass SnapCenter nur einen Initiator pro Host unterstützt.
- Wenn sich die Quelldatenbank oder die Zielinstanz auf einem freigegebenen Clustervolume (CSV) befindet, befindet sich die geklonte Datenbank auf dem CSV.
- Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.



Stellen Sie bei virtuellen Umgebungen (VMDK/RDM) sicher, dass der Einhängepunkt eine dedizierte Festplatte ist.

- 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und dann \* SnapCenter Plug-in für SQL Server\* aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.



Das Klonen einer Sicherung einer Instanz wird nicht unterstützt.

3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** die Sicherung entweder vom primären oder sekundären (gespiegelten oder gewölbten) Speichersystem aus.
5. Wählen Sie die Sicherung aus und wählen Sie dann \*  \*.
6. Führen Sie auf der Seite **Klonoptionen** die folgenden Aktionen aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server klonen      | Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.                                                                                                                                                                                                                                                                                                                                           |
| Instanz klonen     | <p>Wählen Sie eine Kloninstanz aus, auf die Sie die Datenbanksicherung klonen möchten.</p> <p>Diese SQL-Instanz muss sich auf dem angegebenen Klonserver befinden.</p>                                                                                                                                                                                                                                      |
| Klonsuffix         | <p>Geben Sie ein Suffix ein, das an den Namen der Klondatei angehängt wird, um zu kennzeichnen, dass es sich bei der Datenbank um einen Klon handelt.</p> <p>Beispiel: <i>db1_clone</i>. Wenn Sie an denselben Speicherort wie die Originaldatenbank klonen, müssen Sie ein Suffix angeben, um die geklonte Datenbank von der Originaldatenbank zu unterscheiden. Andernfalls schlägt der Vorgang fehl.</p> |

| Für dieses Feld...                                                                       | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mount-Punkt automatisch zuweisen oder Volume-Mount-Punkt automatisch unter Pfad zuweisen | <p>Wählen Sie, ob automatisch ein Bereitstellungspunkt oder ein Volume-Bereitstellungspunkt unter einem Pfad zugewiesen werden soll.</p> <p>Automatische Zuweisung des Volume-Mount-Punkts unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht Ihnen die Angabe eines bestimmten Verzeichnisses. Die Einhängpunkte werden in diesem Verzeichnis erstellt. Bevor Sie diese Option wählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich im Verzeichnis eine Datenbank befindet, befindet sich die Datenbank nach dem Mount-Vorgang in einem ungültigen Zustand.</p> |

7. Wählen Sie auf der Seite „Protokolle“ eine der folgenden Optionen aus:

| Für dieses Feld...              | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Keine                           | Wählen Sie diese Option, wenn Sie nur die vollständige Sicherung ohne Protokolle klonen möchten.                                                                                                                                                                                                                   |
| Alle Protokollsicherungen       | Wählen Sie diese Option, um alle verfügbaren Protokollsicherungen mit einem Datum nach der vollständigen Sicherung zu klonen.                                                                                                                                                                                      |
| Durch Log-Backups bis           | Wählen Sie diese Option, um die Datenbank basierend auf den Sicherungsprotokollen zu klonen, die bis zum Sicherungsprotokoll mit dem ausgewählten Datum erstellt wurden.                                                                                                                                           |
| Nach einem bestimmten Datum bis | <p>Geben Sie das Datum und die Uhrzeit an, nach denen die Transaktionsprotokolle nicht mehr auf die geklonte Datenbank angewendet werden.</p> <p>Dieser Point-in-Time-Klon stoppt den Klon der Transaktionsprotokolleinträge, die nach dem angegebenen Datum und der angegebenen Uhrzeit aufgezeichnet wurden.</p> |

8. Geben Sie auf der Seite **Skript** das Skript-Timeout, den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Klonvorgang ausgeführt werden soll.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

Das Standard-Skript-Timeout beträgt 60 Sekunden.

9. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **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-SmSmtServer“ angegeben haben.

Für EMS finden Sie unter "[Verwalten der EMS-Datenerfassung](#)"

10. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

### Nach Abschluss

Nachdem der Klon erstellt wurde, sollten Sie ihn niemals umbenennen.

### Ähnliche Informationen

["Der Klonvorgang kann mit dem Standardwert TCP\\_TIMEOUT fehlschlagen oder länger dauern"](#)

["Der Datenbankklon der Failover-Cluster-Instanz schlägt fehl"](#)

### PowerShell-Cmdlets

#### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Sicherungen auf, die mit dem Cmdlet Get-SmBackup oder Get-SmResourceGroup geklont werden können.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
C:\PS>PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime              | BackupType  |
|----------|-------------------------------|-------------------------|-------------|
| -----    | -----                         | -----                   | -----       |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015<br>11:02:32 AM | Full Backup |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015<br>11:23:17 AM |             |

In diesem Beispiel werden Informationen zu einer angegebenen Ressourcengruppe, ihren Ressourcen und zugehörigen Richtlinien angezeigt:

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulersSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
ApplySnapvaultUpdate : False  
ApplyRetention : False  
RetentionCount : 0  
RetentionDays : 0  
ApplySnapMirrorUpdate : False  
SnapVaultLabel :  
MirrorVaultUpdateRetryCount : 7  
AppPolicies : {}  
Description : FinancePolicy  
PreScriptPath :  
PreScriptArguments :  
PostScriptPath :  
PostScriptArguments :  
ScriptTimeout : 60000  
DateModified : 8/4/2015 3:43:30 PM  
DateCreated : 8/4/2015 3:43:30 PM  
Schedule : SMCoreContracts.SmSchedule  
PolicyType : Backup  
PluginPolicyType : SMSQL  
Name : FinancePolicy  
Type :  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
clab-a13-13.sddev.lab.netapp.com  
DatabaseGUID :  
SQLInstance : clab-a13-13  
DbStatus : AutoClosed  
DbAccess : eUndefined  
IsSystemDb : False  
IsSimpleRecoveryMode : False  
IsSelectable : True  
SqlDbFileGroups : {}  
SqlDbLogFiles : {}



```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. Starten Sie einen Klonvorgang aus einer vorhandenen Sicherung mithilfe des Cmdlets New-SmClone.

Dieses Beispiel erstellt einen Klon aus einem angegebenen Backup mit allen Protokollen:

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

In diesem Beispiel wird ein Klon einer angegebenen Microsoft SQL Server-Instanz erstellt:

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. Zeigen Sie den Status des Klonauftrags mithilfe des Cmdlets Get-SmCloneReport an.

Dieses Beispiel zeigt einen Klonbericht für die angegebene Job-ID an:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

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"](#) .

## Klon-Lebenszyklus durchführen

Mit SnapCenter können Sie Klone aus einer Ressourcengruppe oder Datenbank erstellen. Sie können entweder einen On-Demand-Klon durchführen oder wiederkehrende Klonvorgänge einer Ressourcengruppe oder Datenbank planen. Wenn Sie regelmäßig ein Backup klonen, können Sie den Klon zum Entwickeln von Anwendungen, Auffüllen von Daten oder Wiederherstellen von Daten verwenden.

Mit SnapCenter können Sie mehrere Klonvorgänge planen, die gleichzeitig auf mehreren Servern ausgeführt werden.

### Bevor Sie beginnen

- Stellen Sie beim Klonen auf eine eigenständige Datenbankinstanz sicher, dass der Mount-Point-Pfad vorhanden ist und es sich um eine dedizierte Festplatte handelt.
- Stellen Sie beim Klonen auf eine Failoverclusterinstanz (FCI) sicher, dass die Bereitstellungspunkte vorhanden sind, es sich um eine gemeinsam genutzte Festplatte handelt und der Pfad und die FCI zur selben SQL-Ressourcengruppe gehören.
- Wenn sich die Quelldatenbank oder die Zielinstanz auf einem freigegebenen Clustervolume (CSV) befindet, befindet sich die geklonte Datenbank auf dem CSV.



Stellen Sie bei virtuellen Umgebungen (VMDK/RDM) sicher, dass der Einhängepunkt eine dedizierte Festplatte ist.

### Informationen zu diesem Vorgang

- Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- Die meisten Felder auf den Seiten des Assistenten „Lebenszyklus klonen“ sind selbsterklärend. Die folgenden Informationen beschreiben Felder, für die Sie möglicherweise Anleitungen benötigen.
- Wenn Sie für ONTAP 9.12.1 und niedrigere Versionen eine Snapshot-Sperrzeit angeben, erben die aus den manipulationssicheren Snapshots erstellten Klone die Ablaufzeit von SnapLock . Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

### 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Ressourcengruppe oder Datenbank aus und klicken Sie dann auf **Lebenszyklus klonen**.
4. Führen Sie auf der Seite „Optionen“ die folgenden Aktionen aus:

| Für dieses Feld...    | Machen Sie Folgendes...                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Name des Klonauftrags | Geben Sie den Namen des Klon-Lebenszyklus-Jobs an, der bei der Überwachung und Änderung des Klon-Lebenszyklus-Jobs hilft.                      |
| Server klonen         | Wählen Sie den Host aus, auf dem der Klon platziert werden soll.                                                                               |
| Instanz klonen        | Wählen Sie die Kloninstanz aus, auf die Sie die Datenbank klonen möchten. Diese SQL-Instanz muss sich auf dem angegebenen Klonserver befinden. |

| Für dieses Feld...                                                                       | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Klonsuffix                                                                               | Geben Sie ein Suffix ein, das an die Klondatenbank angehängt wird, um zu kennzeichnen, dass es sich um einen Klon handelt. Jede SQL-Instanz, die zum Erstellen einer Klon-Ressourcengruppe verwendet wird, muss einen eindeutigen Datenbanknamen haben. Wenn die Klon-Ressourcengruppe beispielsweise eine Quelldatenbank „db1“ aus einer SQL-Instanz „inst1“ enthält und „db1“ nach „inst1“ geklont wird, sollte der Name der Klon-Datenbank „db1clone“ lauten. „clone“ ist ein obligatorisches benutzerdefiniertes Suffix, da die Datenbank auf dieselbe Instanz geklont wird. Wenn „db1“ in die SQL-Instanz „inst2“ geklont wird, kann der Name der Klondatenbank „db1“ bleiben (das Suffix ist optional), da die Datenbank in eine andere Instanz geklont wird. |
| Mount-Punkt automatisch zuweisen oder Volume-Mount-Punkt automatisch unter Pfad zuweisen | Wählen Sie, ob automatisch ein Bereitstellungspunkt oder ein Volumebereitstellungspunkt unter einem Pfad zugewiesen werden soll. Wenn Sie die automatische Zuweisung eines Volume-Mount-Punkts unter einem Pfad auswählen, können Sie ein bestimmtes Verzeichnis angeben. Die Einhängpunkte werden in diesem Verzeichnis erstellt. Bevor Sie diese Option wählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich im Verzeichnis eine Datenbank befindet, befindet sich die Datenbank nach dem Mount-Vorgang in einem ungültigen Zustand.                                                                                                                                                                                                        |

- Wählen Sie auf der Seite „Speicherort“ einen Speicherort aus, um einen Klon zu erstellen.
- Geben Sie auf der Skriptseite den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Klonvorgang ausgeführt werden soll.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

Das Standard-Skript-Timeout beträgt 60 Sekunden.

- Führen Sie auf der Seite „Planen“ eine der folgenden Aktionen aus:
  - Wählen Sie **Jetzt ausführen**, wenn Sie den Klonauftrag sofort ausführen möchten.
  - Wählen Sie **Zeitplan konfigurieren**, wenn Sie festlegen möchten, wie häufig der Klonvorgang erfolgen soll, wann der Klonzeitplan beginnen soll, an welchem Tag der Klonvorgang erfolgen soll, wann der Zeitplan ablaufen soll und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.

- 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-SmSmtServer“ angegeben haben.

Für EMS finden Sie unter ["Verwalten der EMS-Datenerfassung"](#)

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

Sie sollten den Klonvorgang mithilfe der Seite **Überwachen > Jobs** überwachen.

## Überwachen von SQL-Datenbankklonvorgängen

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

- Klicken Sie im linken Navigationsbereich auf **Monitor**.
- Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
- Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
  - Klicken  um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
  - Geben Sie das Start- und Enddatum an.
  - Wählen Sie aus der Dropdownliste **Typ** die Option **Klon** aus.
  - Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
  - Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
- Wählen Sie den Klonauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
- Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

## Abbrechen von SQL-Ressourcenklonvorgängen

Sie können in der Warteschlange befindliche Klonvorgänge abbrechen.

Sie sollten als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Klonvorgänge abzubrechen.

### Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Klonvorgang entweder auf der Seite **Monitor** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Klonvorgänge abzubrechen.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li><li>2. Wählen Sie den Vorgang aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                            |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>1. Klicken Sie nach dem Starten des Klonvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>2. Wählen Sie den Vorgang aus.</li><li>3. Klicken Sie auf der Seite <b>Auftragsdetails</b> auf <b>Auftrag abbrechen</b>.</li></ol> |

## 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 <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme         | Wählen Sie <b>Pfad</b> 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"](#)

# Schützen Sie SAP HANA-Datenbanken

## SnapCenter Plug-in für SAP HANA-Datenbanken

### Übersicht über das SnapCenter -Plug-in für die SAP HANA-Datenbank

Das SnapCenter -Plug-in für SAP HANA-Datenbanken ist eine hostseitige Komponente der NetApp SnapCenter software , die ein anwendungsbewusstes Datenschutzmanagement von SAP HANA-Datenbanken ermöglicht. Das Plug-in für SAP HANA-Datenbanken automatisiert die Sicherung, Wiederherstellung und das Klonen von SAP HANA-Datenbanken in Ihrer SnapCenter Umgebung.

SnapCenter unterstützt Einzelcontainer und Multitenant-Datenbankcontainer (MDC). Sie können das Plug-in für die SAP HANA-Datenbank sowohl in Windows- als auch in Linux-Umgebungen verwenden. Das Plug-In, das nicht auf dem HANA-Datenbankhost installiert ist, wird als zentralisiertes Host-Plug-In bezeichnet. Das zentralisierte Host-Plug-In kann mehrere HANA-Datenbanken auf verschiedenen Hosts verwalten.

Wenn das Plug-in für die SAP HANA-Datenbank installiert ist, können Sie SnapCenter mit der NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen. Sie können das Plug-in auch mit der NetApp SnapVault -Technologie verwenden, um eine Disk-to-Disk-Backup-Replikation zur Einhaltung von Standards durchzuführen.

Das Plug-in für die SAP HANA-Datenbank unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie ein transparentes Failover durchführen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

### Was Sie mit dem SnapCenter Plug-in für die SAP HANA-Datenbank tun können

Wenn Sie das Plug-in für die SAP HANA-Datenbank in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von SAP HANA-Datenbanken und deren Ressourcen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Datenbanken hinzufügen.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

### SnapCenter Plug-in für SAP HANA-Datenbankfunktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit dem Plug-in für die SAP HANA-Datenbank zu



arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter .

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Kopiertechnologie**

SnapCenter verwendet die NetApp Snapshot-Technologie mit dem Plug-in für die SAP HANA-Datenbank zum Sichern von Ressourcen.

Die Verwendung des Plug-ins für die SAP HANA-Datenbank bietet außerdem folgende Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung für die Consistency Group (CG) Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Unterstützung für dateibasierte Sicherung.
- Unterstützung für Linux LVM auf dem XFS-Dateisystem.

## **Vom SnapCenter Plug-in für die SAP HANA-Datenbank unterstützte Speichertypen**

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen Maschinen als auch auf virtuellen Maschinen (VMs). Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter -Plug-in für die SAP HANA-Datenbank installieren.

| Maschine          | Speichertyp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | <ul style="list-style-type: none"> <li>• FC-verbundene LUNs</li> <li>• Über iSCSI verbundene LUNs</li> <li>• Über NFS verbundene Volumes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| VMware ESXi       | <ul style="list-style-type: none"> <li>• RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt.</li> </ul> <p>Sie können die Datei <b>LinuxConfig.pm</b> unter <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> bearbeiten, um den Wert des Parameters <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> auf 1 zu setzen und nur die HBAs erneut zu scannen, die in HBA_DRIVER_NAMES aufgeführt sind.</p> <ul style="list-style-type: none"> <li>• iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind</li> <li>• VMDKs auf NFS-Datenspeichern</li> <li>• VMDKs auf VMFS erstellt</li> <li>• NFS-Volumes, die direkt mit dem Gastsystem verbunden sind</li> <li>• vVol-Datenspeicher auf NFS und SAN</li> </ul> <p>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p> |

## Für das SAP HANA-Plug-In sind mindestens ONTAP Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN erstellen
  - LUN erstellen
  - LUN löschen

- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- LUN-Igroup umbenennen
- lun igroup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN persistent-reservation clear
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen

- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle anzeigen

## Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für SAP HANA-Datenbanken

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#).

## Backup-Strategie für SAP HANA-Datenbanken

### Definieren Sie eine Sicherungsstrategie für SAP HANA-Datenbanken

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge verfügen Sie über die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

### Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

### Schritte

1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.
4. Entscheiden Sie, ob Sie eine auf Snapshot-Kopien basierende Richtlinie erstellen möchten, um anwendungskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie die Integrität der Datenbank überprüfen möchten.
6. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
7. Bestimmen Sie die Aufbewahrungsdauer für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
8. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

### **Automatische Erkennung von Ressourcen auf Linux-Hosts**

Ressourcen sind SAP HANA-Datenbanken und Nicht-Datenvolumes auf dem Linux-Host, die von SnapCenter verwaltet werden. Nach der Installation des SnapCenter -Plug-ins für das SAP HANA-Datenbank-Plug-in werden die SAP HANA-Datenbanken auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.

Die automatische Erkennung wird für die folgenden SAP HANA-Ressourcen unterstützt:

- Einzelbehälter

Nach der Installation oder Aktualisierung des Plug-ins werden die einzelnen Containerressourcen auf einem zentralen Host-Plug-in als manuell hinzugefügte Ressourcen weitergeführt.

Nach der Installation oder Aktualisierung des Plug-Ins werden die SAP HANA-Datenbanken automatisch nur auf den SAP HANA Linux-Hosts erkannt, die direkt bei SnapCenter registriert sind.

- Multitenant-Datenbankcontainer (MDC)

Nach der Installation oder Aktualisierung des Plug-Ins werden die auf einem zentralen Host-Plug-In befindlichen MDC-Ressourcen weiterhin als manuell hinzugefügte Ressourcen verwendet.

Sie müssen die MDC-Ressourcen nach dem Upgrade auf SnapCenter 4.3 weiterhin manuell zum zentralen Host-Plug-In hinzufügen.

Bei SAP HANA Linux-Hosts, die direkt in SnapCenter registriert sind, löst die Installation oder Aktualisierung des Plug-Ins eine automatische Erkennung von Ressourcen auf dem Host aus. Nach dem Upgrade des Plug-Ins wird für jede MDC-Ressource, die sich auf dem Plug-In-Host befand, automatisch eine andere MDC-Ressource mit einem anderen GUID-Format erkannt und in SnapCenter registriert. Die neue Ressource befindet sich im gesperrten Zustand.

Wenn sich beispielsweise in SnapCenter 4.2 eine E90-MDC-Ressource auf dem Plug-In-Host befand und manuell registriert wurde, wird nach dem Upgrade auf SnapCenter 4.3 eine weitere E90-MDC-Ressource mit einer anderen GUID erkannt und in SnapCenter registriert.

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts



Falls die oben genannten Ressourcen erkannt werden, werden die Datenschutzvorgänge für diese Ressourcen nicht unterstützt.

- HANA-Konfiguration mit mehreren Hosts
- Mehrere Instanzen auf demselben Host
- Mehrstufige Scale-Out-HANA-Systemreplikation
- Kaskadierte Replikationsumgebung im Systemreplikationsmodus

## Unterstützte Sicherungstypen

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt dateibasierte Backups und Snapshot-Kopien-basierte Backup-Typen für SAP HANA-Datenbanken.

### Dateibasierte Sicherung

Dateibasierte Backups überprüfen die Integrität der Datenbank. Sie können den dateibasierten Sicherungsvorgang so planen, dass er in bestimmten Intervallen erfolgt. Es werden nur aktive Mandanten gesichert. Sie können dateibasierte Sicherungen von SnapCenter nicht wiederherstellen und klonen.

### Snapshot-Kopie-basierte Sicherung

Auf Snapshot-Kopien basierende Backups nutzen die NetApp Snapshot-Technologie, um schreibgeschützte Online-Kopien der Volumes zu erstellen, auf denen sich die SAP HANA-Datenbanken befinden.

## So verwendet das SnapCenter -Plug-in für die SAP HANA-Datenbank Snapshots der Konsistenzgruppe

Sie können das Plug-In verwenden, um Konsistenzgruppen-Snapshots für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes aufnehmen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe besteht aus gleichzeitigen Snapshots mehrerer Volumes, die konsistente Kopien einer Volumengruppe bereitstellen.

Sie können auch die Wartezeit angeben, die der Speichercontroller benötigt, um Snapshots konsistent zu gruppieren. Die verfügbaren Wartezeitoptionen sind **Dringend**, **Mittel** und **Entspannt**. Sie können die WAFL-Synchronisierung (Write Anywhere File Layout) auch während des konsistenten Gruppen-Snapshot-Vorgangs aktivieren oder deaktivieren. Die WAFL Synchronisierung verbessert die Leistung eines Konsistenzgruppen-Snapshots.

## So verwaltet SnapCenter die Verwaltung von Protokoll- und Datensicherungen

SnapCenter verwaltet die Verwaltung von Protokoll- und Datensicherungen auf Speichersystem- und Dateisystemebene sowie innerhalb des SAP HANA-Sicherungskatalogs.

Die Snapshots auf dem Primär- oder Sekundärspeicher und die entsprechenden Einträge im SAP HANA-Katalog werden basierend auf den Aufbewahrungseinstellungen gelöscht. Beim Sichern und Löschen der Ressourcengruppe werden auch die SAP HANA-Katalogeinträge gelöscht.

## Überlegungen zur Festlegung von Sicherungszeitplänen für die SAP HANA-Datenbank

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen)

Die Sicherungshäufigkeit, bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau wann Backups durchgeführt werden sollen)

Sicherungszeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird.

## Anzahl der für SAP HANA-Datenbanken benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

## Sicherungsnamenskonventionen für Plug-in für SAP HANA-Datenbanken

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

`resourcegroupname_hostname_timestamp`

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.



Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: customtext\_resourcegroup\_policy\_hostname oder resourcegroup\_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

## Wiederherstellungsstrategie für SAP HANA-Datenbanken

### Definieren Sie eine Wiederherstellungsstrategie für SAP HANA-Ressourcen

Sie müssen vor der Wiederherstellung Ihrer Datenbank eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.

#### Schritte

1. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen
2. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken.
3. Entscheiden Sie sich für die Art der Wiederherstellungsvorgänge, die Sie durchführen möchten.

### Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen. Sie können manuell hinzugefügte SAP HANA-Ressourcen nicht wiederherstellen.



Sie können manuell hinzugefügte SAP HANA-Ressourcen nicht wiederherstellen.

### Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

### Wiederherstellung auf Dateiebene

- Stellt Dateien aus Volumes, Qtrees oder Verzeichnissen wieder her
- Stellt nur die ausgewählten LUNs wieder her

### Unterstützte Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für automatisch erkannte SAP HANA-Datenbanken.

## Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her
  - Um das gesamte Volume wiederherzustellen, sollte die Option **Volume Revert** ausgewählt werden.



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

## Mandantendatenbank

- Stellt die Mandantendatenbank wieder her

Wenn die Option **Mandantendatenbank** ausgewählt ist, müssen für die Durchführung des Wiederherstellungsvorgangs externe HANA-Studio- oder HANA-Wiederherstellungsskripte von SnapCenter verwendet werden.

## Arten von Wiederherstellungsvorgängen für automatisch erkannte SAP HANA-Datenbanken

SnapCenter unterstützt Volume-basiertes SnapRestore (VBSR), Single File SnapRestore und Connect-and-Copy-Wiederherstellungstypen für automatisch erkannte SAP HANA-Datenbanken.

**Volume-basiertes SnapRestore (VBSR) wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:**

- Wenn die für die Wiederherstellung ausgewählte Sicherung auf Versionen vor SnapCenter 4.3 erstellt wird und nur, wenn die Option **Ressource vollständig** ausgewählt ist
- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und die Option **Volume Revert** ausgewählt ist

**Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:**

- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und nur die Option **Complete Resource** ausgewählt ist
- Für Multitenant-Datenbankcontainer (MDC), wenn die für die Wiederherstellung ausgewählte Sicherung auf SnapCenter 4.3 erstellt wird und die Option **Tenant-Datenbank** ausgewählt ist
- Wenn das ausgewählte Backup von einem SnapMirror oder SnapVault Sekundärspeicherort stammt und die Option **Complete Resource** ausgewählt ist

**Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien durchgeführt:**

- Wenn Backups auf Versionen vor SnapCenter 4.3 erstellt werden und nur, wenn die Option **Complete Resource** ausgewählt ist
- Wenn Backups in SnapCenter 4.3 erstellt werden und nur, wenn die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem SnapMirror oder SnapVault Sekundärspeicherort ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Eine auf Verbinden und Kopieren basierende Wiederherstellung wird in SAN-Umgebungen für das folgende Szenario durchgeführt:

- Für MDC, wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und die Option **Tenant Database** ausgewählt ist



Auf der Seite „Wiederherstellungsbereich“ sind die Optionen „Ressource vollständig“ und „Volume wiederherstellen“ verfügbar.

### Für SAP HANA-Datenbanken unterstützte Arten von Wiederherstellungsvorgängen

Mit SnapCenter können Sie verschiedene Arten von Wiederherstellungsvorgängen für SAP HANA-Datenbanken durchführen.

- Wiederherstellen der Datenbank bis zum aktuellsten Stand
- Wiederherstellen der Datenbank bis zu einem bestimmten Zeitpunkt

Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.

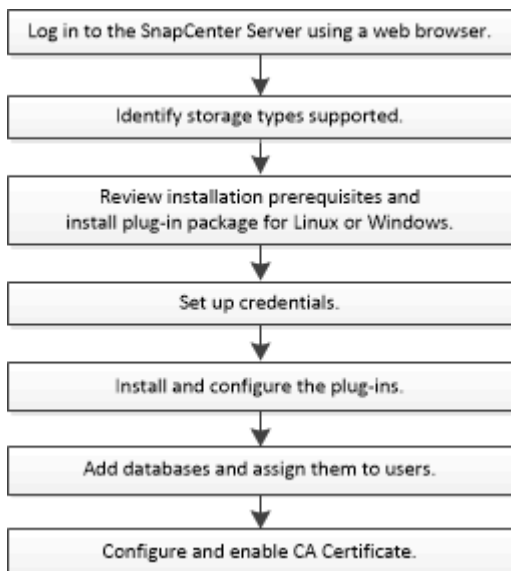
- Wiederherstellen der Datenbank bis zu einer bestimmten Datensicherung

SnapCenter bietet auch die Option „Keine Wiederherstellung“ für SAP HANA-Datenbanken.

## Vorbereiten der Installation des SnapCenter Plug-ins für die SAP HANA-Datenbank

### Installationsworkflow des SnapCenter Plug-ins für die SAP HANA-Datenbank

Sie sollten das SnapCenter Plug-in für die SAP HANA-Datenbank installieren und einrichten, wenn Sie SAP HANA-Datenbanken schützen möchten.



## Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter -Plug-ins für die SAP HANA-Datenbank

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Das SnapCenter Plug-in für die SAP HANA-Datenbank ist sowohl in Windows- als auch in Linux-Umgebungen verfügbar.

- Sie müssen Java 11 auf Ihrem Host installiert haben.



IBM Java wird auf Windows- und Linux-Hosts nicht unterstützt.

- Sie müssen das interaktive SAP HANA-Datenbankterminal (HDBSQL-Client) auf dem Host installiert haben.
- Unter Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „LocalSystem“ ausgeführt werden. Dies ist das Standardverhalten, wenn das Plug-in für die SAP HANA-Datenbank als Domänenadministrator installiert wird.
- Unter Windows sollten Benutzerspeicherschlüssel als SYSTEM-Benutzer erstellt werden.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren. Das SnapCenter -Plug-in für Microsoft Windows wird standardmäßig mit dem SAP HANA-Plug-in auf Windows-Hosts bereitgestellt.
- Bei Linux-Hosts erfolgt der Zugriff auf die Schlüssel des HDB Secure User Store als HDBSQL-Betriebssystembenutzer.
- Der SnapCenter -Server sollte Zugriff auf den 8145- oder benutzerdefinierten Port des Plug-ins für den SAP HANA-Datenbankhost haben.

### Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Während der Installation des Plug-ins für die SAP HANA-Datenbank auf einem Windows-Host wird das SnapCenter Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Windows-Host installiert haben.

["Laden Sie JAVA für alle Betriebssysteme herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

### Linux-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

["Laden Sie JAVA für alle Betriebssysteme herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Bei SAP HANA-Datenbanken, die auf einem Linux-Host ausgeführt werden, wird bei der Installation des

Plug-ins für die SAP HANA-Datenbank automatisch das SnapCenter Plug-in für UNIX installiert.

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

## Ergänzende Befehle

Um einen zusätzlichen Befehl im SnapCenter -Plug-in für SAP HANA auszuführen, müssen Sie ihn in die Datei *allowed\_commands.config* aufnehmen.

- Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/NetApp/snapcenter/scc/etc/allowed\_commands.config*

Um zusätzliche Befehle auf dem Plug-In-Host zuzulassen, öffnen Sie die Datei *allowed\_commands.config* in einem Editor. Geben Sie jeden Befehl in einer separaten Zeile ein. Bei den Befehlen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen (") einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: mount

Befehl: umount

Befehl: "C:\Programme\NetApp\SnapCreator commands\sdcli.exe"

Befehl: myscript.bat

Wenn die Datei *allowed\_commands.config* nicht vorhanden ist, werden die Befehle oder die Skriptausführung blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."

Wenn der Befehl oder das Skript nicht in der Datei „*allowed\_commands.config*“ vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."



Um alle Befehle zuzulassen, sollten Sie keinen Platzhaltereintrag (\*) verwenden.

## Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host

SnapCenter 2.0 und spätere Versionen ermöglichen es einem Nicht-Root-Benutzer, das SnapCenter -Plug-In -Paket für Linux zu installieren und den Plug-In-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

## Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.

- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/bin/spl`

## Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei `/etc/sudoers` hinzu.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „/`<crs_home>`/bin/olsnodes“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`LINUX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den Prüfsummenwert aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist. .



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>5 GB</p> <div>  <p>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.</p> </div>                                                                                         |
| Erforderliche Softwarepakete                                                                 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java und OpenJDK</li> </ul> <p>Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

## Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux

Bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren, sollten Sie mit einigen grundlegenden Anforderungen an Speicherplatz und Größe des Hostsystems vertraut sein.



| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                                                                     |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>2 GB</p> <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | <p>Java 11 Oracle Java und OpenJDK</p> <p>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.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                              |

## Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für die SAP HANA-Datenbank

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Datenbanken oder Windows-Dateisystemen erstellen.

### Informationen zu diesem Vorgang

- Linux-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldeinformationen für den Root-Benutzer oder für einen Nicht-Root-Benutzer mit Sudo-Berechtigungen einrichten, um den Plug-In-Prozess zu installieren und zu starten.

**Best Practice:** Obwohl Sie Anmeldeinformationen für Linux erstellen dürfen, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

- Windows-Hosts

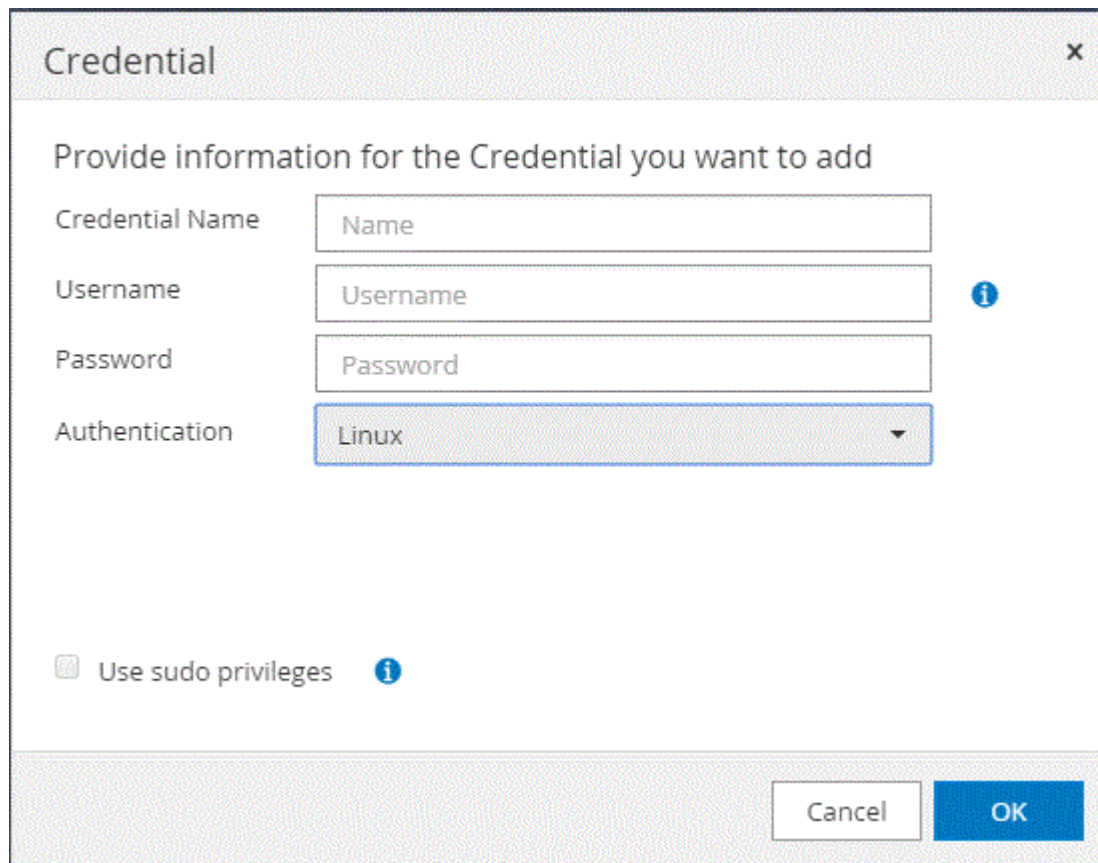
Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.

Sie müssen die Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.



4. Geben Sie auf der Seite „Anmeldeinformationen“ die zum Konfigurieren der Anmeldeinformationen erforderlichen Informationen an:

| Für dieses Feld...      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Benutzername            | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i></p> <p>Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (&lt;) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als &lt;!10, kleiner als 10 &lt;!, Backtick `12.</p> |
| Passwort                | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Authentifizierungsmodus | Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen <b>Sudo-Berechtigungen verwenden</b>, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p> <p> Gilt nur für Linux-Benutzer.</p> |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

## Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

### Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -Effectivelmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des
Dienstkontos.
```

#### 4. Konfigurieren Sie das gMSA auf Ihren Hosts:

- a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                |
|---------|----------------|-----------|-----------------------------------------------|
| -----   | -----          | -----     | -----                                         |
| True    | No             | Success   | {Active Directory Domain Services, Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Starten Sie Ihren Host neu.
  - b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
  - c. Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Installieren Sie das SnapCenter -Plug-in für SAP HANA-Datenbanken

### Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren.

**Bevor Sie beginnen**

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zur Verwaltung von Hosts.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

["Konfigurieren eines gruppenverwalteten Dienstkontos unter Windows Server 2016 oder höher für SAP HANA"](#)

### Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Damit die SAP HANA-Systemreplikation Ressourcen sowohl auf primären als auch auf sekundären Systemen erkennt, wird empfohlen, sowohl das primäre als auch das sekundäre System mithilfe des Root- oder Sudo-Benutzers hinzuzufügen.

### 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            | <p>Wählen Sie den Hosttyp aus:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> </ul> <div>  <p>Das Plug-in für SAP HANA wird auf dem HDBSQL-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> </div> |

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hostname             | <p>Geben Sie den Hostnamen für die Kommunikation ein. Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p> <p>Sie müssen den HDBSQL-Client und HDBUserStore auf diesem Host konfigurieren.</p>                                                                                                                                                                                                                                                                                                                                                           |
| Anmeldeinformationen | <p>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.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div>  <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

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

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen              | <p>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.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installationspfad                                                                           | <p>Das Plug-in für SAP HANA wird auf dem HDBSQL-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> <ul style="list-style-type: none"> <li>Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter. Optional können Sie den Pfad anpassen.</li> <li>Für das SnapCenter Plug-ins-Paket für Linux ist der Standardpfad /opt/ NetApp/snapcenter. Optional können Sie den Pfad anpassen.</li> </ul>                                                                                  |
| Vorinstallationsprüfungen überspringen                                                      | 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.                                                                                                                                                                                                                                                                                                                                                                    |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | <p>Aktivieren Sie für Windows-Hosts dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.</p> <div>  <p>Geben Sie den gMSA-Namen im folgenden Format an:<br/>Domänenname\Kontoname\$.</p> </div> <div>  <p>gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.</p> </div> |

7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-Ins) und Java-Version (für Linux-Plug-Ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, 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, müssen Sie das Problem beheben.



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

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.



In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



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`.

### **Installieren Sie SnapCenter Plug-in-Pakete für Linux oder Windows auf mehreren Remote-Hosts mithilfe von Cmdlets**

Sie können die SnapCenter -Plug-in-Pakete für Linux oder Windows mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

#### **Bevor Sie beginnen**

Sie müssen sich auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

#### **Schritte**

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-In auf mehreren Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

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"](#) .

Sie können die Option `-skippercheck` verwenden, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

### **Installieren Sie das SnapCenter -Plug-in für die SAP HANA-Datenbank auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle**

Sie sollten das SnapCenter Plug-in für die SAP HANA-Datenbank mithilfe der SnapCenter Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie das Plug-In für die SAP HANA-Datenbank entweder im Konsolenmodus oder im unbeaufsichtigten Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

#### **Bevor Sie beginnen**

- Sie sollten das Plug-in für die SAP HANA-Datenbank auf jedem Linux-Host installieren, auf dem sich der HDBSQL-Client befindet.
- Der Linux-Host, auf dem Sie das SnapCenter -Plug-in für die SAP HANA-Datenbank installieren, muss die abhängigen Software-, Datenbank- und Betriebssystemanforderungen erfüllen.

Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den unterstützten Konfigurationen.

<https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT>

- Das SnapCenter -Plug-in für die SAP HANA-Datenbank ist Teil des SnapCenter Plug-in-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins-Paket für Linux installieren, sollten Sie SnapCenter bereits auf einem Windows-Host installiert haben.

## Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter Plug-ins-Pakets für Linux (snapcenter\_linux\_host\_plugin.bin) von C:\ProgramData\NetApp\ SnapCenter\Package Repository auf den Host, auf dem Sie das Plug-in für die SAP HANA-Datenbank installieren möchten.

Sie können auf diesen Pfad von dem Host aus zugreifen, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei kopiert haben.

3. Installieren Sie das Plug-In:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT gibt den SMCore HTTPS-Kommunikationsport an.
- -DSERVER\_IP gibt die IP-Adresse des SnapCenter -Servers an.
- -DSERVER\_HTTPS\_PORT gibt den HTTPS-Port des SnapCenter -Servers an.
- -DUSER\_INSTALL\_DIR gibt das Verzeichnis an, in dem Sie das SnapCenter Plug-Ins-Paket für Linux installieren möchten.
- DINSTALL\_LOG\_NAME gibt den Namen der Protokolldatei an.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Bearbeiten Sie die Datei /<Installationsverzeichnis>/NetApp/snapcenter/scc/etc/SC\_SMS\_Services.properties und fügen Sie dann den Parameter PLUGINS\_ENABLED = hana:3.0 hinzu.
5. Fügen Sie den Host mit dem Cmdlet Add-Smhost und den erforderlichen Parametern zum SnapCenter -Server hinzu.

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 "[Referenzhandbuch für SnapCenter -Software-Cmdlets](#)".

## Überwachen Sie den Status der Installation des Plug-ins für SAP HANA

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

## CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

## Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

## Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
  - a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

*Get-ChildItem -Pfad Zertifikat:\LocalMachine\My*

- b. Kopieren Sie den Fingerabdruck.

## Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

## Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-
in-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## Konfigurieren Sie das CA-Zertifikat für den SnapCenter SAP HANA Plug-Ins-Dienst auf dem Linux-Host

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

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter `/opt/NetApp/snapcenter/scc/etc` befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Dies ist der Wert, der dem Schlüssel „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_in_cert" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE\_PASS in der Datei *agent.properties*.

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



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

## Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

## Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: /opt/ NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder  
Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

## Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/ NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE\_PASS in der Datei agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks  
. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei  
agent.properties.
```

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC\_CERTIFICATE\_ALIAS.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

#### Informationen zu diesem Vorgang

- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-Ins ist „opt/NetApp/snapcenter/scc/etc/crl“.

#### Schritte

1. Sie können das Standardverzeichnis in der Datei agent.properties anhand des Schlüssels CRL\_PATH ändern und aktualisieren.

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

### Konfigurieren Sie das CA-Zertifikat für den SnapCenter SAP HANA Plug-Ins-Dienst auf dem Windows-Host

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

Die Plug-Ins verwenden die Datei *keystore.jks*, die sich unter *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

#### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-



Agenten abrufen.

Es handelt sich um den Wert, der dem Schlüssel *KEYSTORE\_PASS* entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

```
C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

```
keytool -keypasswd -alias "Aliasname_im_Zertifikat" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel *KEYSTORE\_PASS* in der Datei *agent.properties*.

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



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

#### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

##### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

##### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher `C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. Suchen Sie die Datei `keystore.jks`.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels `KEYSTORE_PASS` in der Datei `agent.properties`.

```
keytool -keypasswd -alias "Aliasname_im_CA_Zertifikat" -keystore keystore.jks
```

8. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei `agent.properties`.

Aktualisieren Sie diesen Wert anhand des Schlüssels `SCC_CERTIFICATE_ALIAS`.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

## Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter -Plug-Ins

### Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe ["So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat"](#) .
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist `'C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\crl'`.

### Schritte

1. Sie können das Standardverzeichnis in der Datei `agent.properties` anhand des Schlüssels `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 Datenschutz vor

### Voraussetzungen für die Verwendung des SnapCenter Plug-ins für SAP HANA-Datenbank

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

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich beim SnapCenter -Server an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen und gegebenenfalls Anmeldeinformationen erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

Sie müssen den Java-Pfad in der Umgebungspfadvariable des Hostcomputers festlegen.

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.
- Installieren Sie den HDBSQL-Client auf dem Host, auf dem Sie das Plug-in für die SAP HANA-Datenbank installieren.

Konfigurieren Sie die Benutzerspeicherschlüssel für die SAP HANA-Knoten, die Sie über diesen Host verwalten.

- Wenn Sie für die SAP HANA-Datenbank 2.0SPS05 ein SAP HANA-Datenbankbenutzerkonto verwenden, stellen Sie sicher, dass Sie über die folgenden Berechtigungen zum Durchführen von Sicherungs-, Wiederherstellungs- und Klonvorgängen in SnapCenter Server verfügen:
  - Backup-Administrator
  - Katalog gelesen
  - Datenbank-Backup-Administrator
  - Datenbankwiederherstellungsoperator

### So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SAP HANA-Datenbanken verwendet

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei den Ressourcen handelt es sich typischerweise um SAP HANA-Datenbanken, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Sicherungshäufigkeit, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

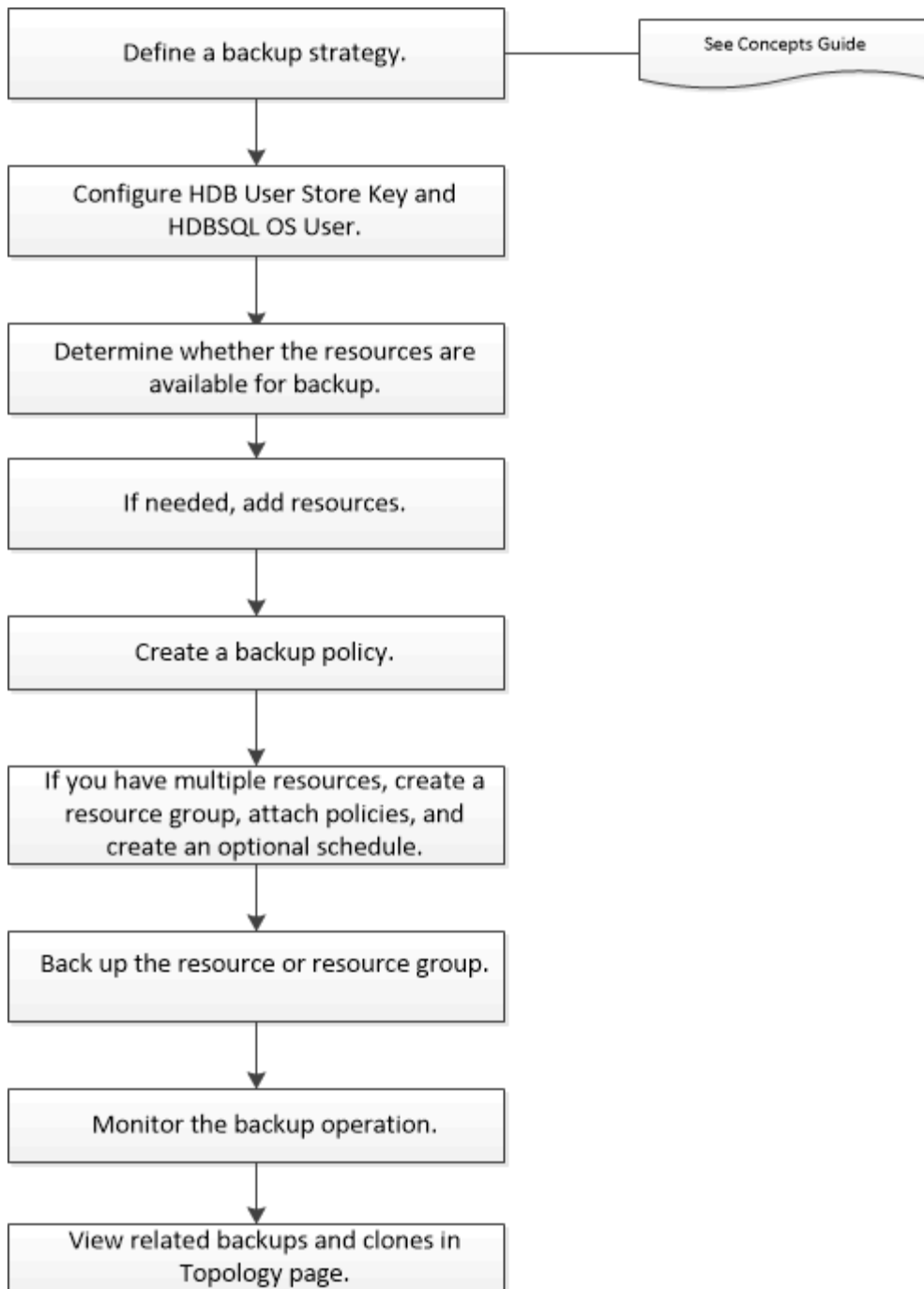
Stellen Sie sich eine Ressourcengruppe so vor, dass sie definiert, was Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als ob sie definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken im Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird.

## **Sichern von SAP HANA-Ressourcen**

### **Sichern von SAP HANA-Ressourcen**

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Sicherungsworkflow umfasst die Planung, die Identifizierung der zu sichernden Datenbanken, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets. ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Konfigurieren Sie den HDB User Store Key und den HDBSQL OS User für die SAP HANA-Datenbank

Sie müssen den HDB User Store Key und den HDBSQL OS User konfigurieren, um Datenschutzvorgänge für SAP HANA-Datenbanken durchzuführen.

**Bevor Sie beginnen**

- Wenn für die SAP HANA-Datenbank der HDB Secure User Store Key und der HDB SQL OS User nicht konfiguriert sind, wird nur für die automatisch erkannten Ressourcen ein rotes Vorhängeschlosssymbol angezeigt. Wenn sich bei einem nachfolgenden Erkennungsvorgang herausstellt, dass der konfigurierte HDB Secure User Store Key falsch ist oder keinen Zugriff auf die Datenbank selbst gewährt, wird das rote Vorhängeschlosssymbol erneut angezeigt.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS-Benutzer konfigurieren, um die Datenbank schützen zu können, oder sie einer Ressourcengruppe hinzufügen, um Datenschutzvorgänge durchzuführen.
- Sie müssen den HDB SQL OS-Benutzer konfigurieren, um auf die Systemdatenbank zugreifen zu können. Wenn der HDB SQL OS-Benutzer so konfiguriert ist, dass er nur auf die Mandantendatenbank zugreift, schlägt der Erkennungsvorgang fehl.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann SnapCenter Plug-in für SAP HANA-Datenbank aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste **Anzeigen** aus.
3. (Optional) Klicken Sie auf  und wählen Sie den Hostnamen aus.

Sie können dann auf , um den Filterbereich zu schließen.

4. Wählen Sie die Datenbank aus und klicken Sie dann auf **Datenbank konfigurieren**.
5. Geben Sie im Abschnitt „Datenbankeinstellungen konfigurieren“ den HDB Secure User Store Key ein.



Der Plug-in-Hostname wird angezeigt und der HDB SQL OS-Benutzer wird automatisch mit <sid>adm ausgefüllt.

6. Klicken Sie auf **OK**.

Sie können die Datenbankkonfiguration auf der Seite „Topologie“ ändern.

## Ermitteln Sie Ressourcen und bereiten Sie Multitenant-Datenbankcontainer für den Datenschutz vor

### Automatisches Erkennen der Datenbanken

Ressourcen sind SAP HANA-Datenbanken und Nicht-Datenvolumes auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren SAP HANA-Datenbanken ermittelt haben.

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen des HDB User Store Key, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen abgeschlossen haben.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS-Benutzer auf dem Linux-Host konfiguriert haben.
  - Sie müssen den HDB-Benutzerspeicherschlüssel mit der SID „Adm-Benutzer“ konfigurieren. Beispielsweise muss für ein HANA-System mit A22 als SID der HDB-Benutzerspeicherschlüssel mit a22adm konfiguriert werden.

- Das SnapCenter Plug-in für die SAP HANA-Datenbank unterstützt keine automatische Erkennung der in virtuellen RDM/VMDK-Umgebungen vorhandenen Ressourcen. Sie müssen die Speicherinformationen für virtuelle Umgebungen angeben, während Sie die Datenbanken manuell hinzufügen.

### Informationen zu diesem Vorgang

Nach der Installation des Plug-Ins werden alle Ressourcen auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.

Die automatisch erkannten Ressourcen können nicht geändert oder gelöscht werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für die SAP HANA-Datenbank aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste „Anzeigen“ aus.
3. (Optional) Klicken Sie auf  \* und wählen Sie dann den Hostnamen aus.

Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen anzuzeigen.

Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp -Speichersystem befindet und geschützt ist und kein Sicherungsvorgang ausgeführt wird, wird in der Spalte „Gesamtstatus“ die Meldung „Sicherung nicht ausgeführt“ angezeigt. Andernfalls ändert sich der Status basierend auf dem letzten Sicherungsstatus in „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“.



Wenn für die SAP HANA-Datenbank kein HDB Secure User Store Key konfiguriert ist, wird neben der Ressource ein rotes Vorhängeschlosssymbol angezeigt. Wenn sich bei einem nachfolgenden Erkennungsvorgang herausstellt, dass der konfigurierte HDB Secure User Store Key falsch ist oder keinen Zugriff auf die Datenbank selbst gewährt, wird das rote Vorhängeschlosssymbol erneut angezeigt.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

### Nach Abschluss

Sie müssen den HDB Secure User Store Key und den HDBSQL OS User konfigurieren, um die Datenbank schützen zu können, oder sie der Ressourcengruppe hinzufügen, um Datenschutzvorgänge durchzuführen.

["Konfigurieren Sie den HDB User Store Key und den HDBSQL OS User für die SAP HANA-Datenbank"](#)

### Vorbereiten von Multitenant-Datenbankcontainern für den Datenschutz

Bei SAP HANA-Hosts, die direkt in SnapCenter registriert sind, löst die Installation oder Aktualisierung des SnapCenter -Plug-Ins für die SAP HANA-Datenbank eine automatische Erkennung von Ressourcen auf dem Host aus. Nach der Installation oder Aktualisierung des Plug-Ins wird für jede Multitenant-Datenbankcontainer-Ressource



(MDC), die sich auf dem Plug-In-Host befand, automatisch eine andere MDC-Ressource mit einem anderen GUID-Format erkannt und in SnapCenter registriert. Die neue Ressource befindet sich im Status „gesperrt“.

### Informationen zu diesem Vorgang

Wenn sich beispielsweise in SnapCenter 4.2 eine E90-MDC-Ressource auf dem Plug-In-Host befand und manuell registriert wurde, wird nach dem Upgrade auf SnapCenter 4.3 eine weitere E90-MDC-Ressource mit einer anderen GUID erkannt und in SnapCenter registriert.



Die mit der Ressource von SnapCenter 4.2 und früheren Versionen verbundenen Backups müssen bis zum Ablauf der Aufbewahrungsfrist aufbewahrt werden. Nach Ablauf der Aufbewahrungsfrist können Sie die alte MDC-Ressource löschen und mit der Verwaltung der neuen automatisch erkannten MDC-Ressource fortfahren.

„Old MDC resource“ ist die MDC-Ressource für einen Plug-In-Host, der in SnapCenter 4.2 oder früheren Versionen manuell hinzugefügt wurde.

Führen Sie die folgenden Schritte aus, um die in SnapCenter 4.3 entdeckte neue Ressource für Datenschutzvorgänge zu verwenden:

### Schritte

1. Wählen Sie auf der Seite „Ressourcen“ die alte MDC-Ressource mit den Sicherungen aus, die der früheren SnapCenter Version hinzugefügt wurden, und versetzen Sie sie auf der Seite „Topologie“ in den „Wartungsmodus“.

Wenn die Ressource Teil einer Ressourcengruppe ist, versetzen Sie die Ressourcengruppe in den „Wartungsmodus“.

2. Konfigurieren Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie die neue Ressource auf der Seite „Ressourcen“ auswählen.

„Neue MDC-Ressource“ ist die neu entdeckte MDC-Ressource, die entdeckt wurde, als der SnapCenter -Server und der Plug-In-Host auf 4.3 aktualisiert wurden. Die neue MDC-Ressource kann für einen bestimmten Host als Ressource mit derselben SID wie die alte MDC-Ressource und auf der Ressourcenseite mit einem roten Vorhängeschlosssymbol daneben identifiziert werden.

3. Schützen Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie Schutzrichtlinien, Zeitpläne und Benachrichtigungseinstellungen auswählen.
4. Löschen Sie die in SnapCenter 4.2 oder früheren Versionen erstellten Sicherungen basierend auf den Aufbewahrungseinstellungen.
5. Löschen Sie die Ressourcengruppe von der Seite „Topologie“.
6. Löschen Sie die alte MDC-Ressource von der Ressourcenseite.

Wenn beispielsweise die Aufbewahrungsdauer für primäre Snapshots 7 Tage und die für sekundäre Snapshots 45 Tage beträgt, müssen Sie nach Ablauf der 45 Tage und nachdem alle Sicherungen gelöscht wurden, die Ressourcengruppe und die alte MDC-Ressource löschen.

### Ähnliche Informationen

["Konfigurieren Sie den HDB User Store Key und den HDBSQL OS User für die SAP HANA-Datenbank"](#)

["Anzeigen von SAP HANA-Datenbanksicherungen und -klonen auf der Seite „Topologie“"](#)

## Ressourcen manuell zum Plug-In-Host hinzufügen

Die automatische Erkennung wird für bestimmte HANA-Instanzen nicht unterstützt. Sie müssen diese Ressourcen manuell hinzufügen.

### Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen des HDB-Benutzerspeicherschlüssels abgeschlossen haben.
- Für die SAP HANA-Systemreplikation wird empfohlen, alle Ressourcen dieses HANA-Systems zu einer Ressourcengruppe hinzuzufügen und eine Sicherung der Ressourcengruppe zu erstellen. Dadurch wird eine nahtlose Sicherung während des Übernahme-Failback-Modus gewährleistet.

["Erstellen von Ressourcengruppen und Anfügen von Richtlinien"](#) .

### Informationen zu diesem Vorgang

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts



Falls die oben genannten Ressourcen erkannt werden, werden die Datenschutzvorgänge für diese Ressourcen nicht unterstützt.

- HANA-Konfiguration mit mehreren Hosts
- Mehrere Instanzen auf demselben Host
- Mehrstufige Scale-Out-HANA-Systemreplikation
- Kaskadierte Replikationsumgebung im Systemreplikationsmodus

### Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter -Plug-in für die SAP HANA-Datenbank aus der Dropdown-Liste aus und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite „Ressourcen“ auf **SAP HANA-Datenbank hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ressourcentyp      | Geben Sie den Ressourcentyp ein. Ressourcentypen sind Einzelcontainer, Multitenant-Datenbankcontainer (MDC) und Nicht-Datenvolumen.                                    |
| HANA-Systemname    | Geben Sie den beschreibenden SAP HANA-Systemnamen ein. Diese Option ist nur verfügbar, wenn Sie die Ressourcentypen „Einzelner Container“ oder „MDC“ ausgewählt haben. |
| SID                | Geben Sie die System-ID (SID) ein. Das installierte SAP HANA-System wird durch eine einzelne SID identifiziert.                                                        |

| Für dieses Feld...              | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plug-in-Host                    | Wählen Sie den Plug-In-Host aus.                                                                                                                                                                                                                                                                                        |
| HDB Secure User Store-Schlüssel | <p>Geben Sie den Schlüssel ein, um eine Verbindung zum SAP HANA-System herzustellen.</p> <p>Der Schlüssel enthält die Anmeldeinformationen zur Verbindung mit der Datenbank.</p> <p>Bei der SAP HANA-Systemreplikation wird der sekundäre Benutzerschlüssel nicht validiert. Dies wird bei der Übernahme verwendet.</p> |
| HDBSQL OS-Benutzer              | Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist. Unter Windows muss der HDBSQL-Betriebssystembenutzer zwingend der SYSTEM-Benutzer sein. Daher müssen Sie den HDB Secure User Store Key für den SYSTEM-Benutzer konfigurieren.                                                  |

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ ein Speichersystem und ein oder mehrere Volumes, LUNs und Qtrees aus und klicken Sie dann auf **Speichern**.

Optional: Sie können auf das \* klicken  \* Symbol zum Hinzufügen weiterer Volumes, LUNs und Qtrees aus anderen Speichersystemen.

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

Die Datenbanken werden zusammen mit Informationen wie SID, Plug-In-Host, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie die Ressourcen den Benutzern zuweisen. Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

["Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"](#)

Nachdem Sie die Datenbanken hinzugefügt haben, können Sie die Details der SAP HANA-Datenbank ändern.

Folgendes können Sie nicht ändern, wenn mit der SAP HANA-Ressource Sicherungen verknüpft sind:

- Multitenant-Datenbankcontainer (MDC): SID oder HDBSQL-Client (Plug-In)-Host
- Einzelner Container: SID oder HDBSQL-Client (Plug-In)-Host
- Nicht-Datenvolumen: Ressourcename, zugehörige SID oder Plug-in-Host

## Erstellen von Sicherungsrichtlinien für SAP HANA-Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden,

müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren.

### Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für SAP HANA-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen von Ressourcen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

Darüber hinaus können Sie in der Richtlinie Replikations-, Skript- und Anwendungseinstellungen angeben. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

- 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

- SAP HANA-Systemreplikation
  - Sie können das primäre SAP HANA-System schützen und alle Datenschutzvorgänge durchführen.
  - Sie können das sekundäre SAP HANA-System schützen, aber die Sicherungen können nicht erstellt werden.

Nach dem Failover können alle Datenschutzvorgänge durchgeführt werden, da das sekundäre SAP HANA-System zum primären SAP HANA-System wird.

Sie können kein Backup für das SAP HANA-Datenvolumen erstellen, aber SnapCenter schützt weiterhin die Nicht-Datenvolumes (NDV).

- 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. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - Speichertyp auswählen
  - Wählen Sie den Sicherungstyp:

| Wenn Sie wollen...                                     | Machen Sie Folgendes...                                                             |
|--------------------------------------------------------|-------------------------------------------------------------------------------------|
| Erstellen Sie ein Backup mit der Snapshot-Technologie  | Wählen Sie <b>Snapshot-basiert</b> .                                                |
| Führen Sie eine Integritätsprüfung der Datenbank durch | Wählen Sie <b>Dateibasiertes Backup</b> . Es werden nur aktive Mandanten gesichert. |

6. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:
  - Geben Sie den Zeitplantyp an, indem Sie **Auf Anfrage, Stündlich, Täglich, Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber auch jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

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



| Wenn Sie wollen...                               | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Snapshots | <p data-bbox="841 155 1484 256">Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p data-bbox="841 289 1484 390">Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden zuerst die ältesten Snapshots gelöscht.</p> <div data-bbox="873 436 1484 1474"> <div data-bbox="873 436 1484 655">  <p data-bbox="987 436 1484 655">Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der ONTAP Version unterstützt wird.</p> </div> <div data-bbox="873 688 1484 1159">  <p data-bbox="987 688 1484 1159">Für Snapshot-Kopien-basierte Backups müssen Sie 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.</p> </div> <div data-bbox="873 1192 1484 1474">  <p data-bbox="987 1192 1484 1474">Für die SAP HANA-Systemreplikation wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. Dadurch wird sichergestellt, dass die richtige Anzahl an Sicherungen aufbewahrt wird.</p> </div> </div> |

| Wenn Sie wollen...                                                 | Dann...                                                                                                                                                                         |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> 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 <b>Sperrzeitraum für Snapshot-Kopien</b> und geben Sie Tage, Monate oder Jahre an.<br><br>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen. |

8. Wählen Sie eine Snapshot-Bezeichnung 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.

SAP HANA-Systemreplikation und der sekundären SAP HANA-Systemreplikation auf 7 festgelegt.

Sie können maximal 7 Snapshots gleichzeitig erstellen, sowohl die primäre als auch die sekundäre SAP HANA-Systemreplikation.

9. Wählen Sie für auf Snapshot-Kopien basierende Sicherungen im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:



| Für dieses Feld...                                                                                 | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b></p> | <p>Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation).</p> <p>Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.</p> <p>Wenn die Schutzbeziehung in ONTAP vom Typ „Mirror und Vault“ ist und Sie nur diese Option auswählen, wird der auf dem primären Server erstellte Snapshot nicht an das Ziel übertragen, sondern im Ziel aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird die Fehlermeldung „Der sekundäre Speicherort ist für die ausgewählte gewölbte/gespiegelte Sicherung nicht verfügbar“ angezeigt.</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen von SAP HANA-Datenbanksicherungen und -klonen auf der Seite „Topologie“"</a> .</p> |

| Für dieses Feld...                                                                         | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b> | <p>Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.</p> <p>Weitere Informationen zu SnapLock Vault finden Sie unter <a href="#">"Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel"</a></p> <p>Sehen <a href="#">"Anzeigen von SAP HANA-Datenbanksicherungen und -klonen auf der Seite „Topologie“"</a> .</p> |
| <b>Fehler bei der Wiederholungsanzahl</b>                                                  | Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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

## Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### Informationen zu diesem Vorgang

- Um Backups der SAP HANA-Systemreplikation zu erstellen, wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. Dadurch wird eine nahtlose Sicherung während

des Übernahme-Failback-Modus gewährleistet.

- 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.
- Das Hinzufügen neuer Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken 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. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann 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:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | <p>Geben Sie einen Namen für die Ressourcengruppe ein.</p> <div> Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</div>                                                                                                           |
| Schlagwörter                                                  | <p>Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.</p> <p>Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.</p>                                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | <p>Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.</p> <p>Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p> |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

Dies hilft, Informationen auf dem Bildschirm zu filtern.

5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den

Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.

6. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Consistency Group Snapshot-Vorgangs zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs anzugeben.<br><br>Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                         | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

+

a. Klicken Sie auf den Pfeil **Skripts** und geben Sie 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.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

| Parameter         | Einstellung | Beschreibung                                                              |
|-------------------|-------------|---------------------------------------------------------------------------|
| ARCHIV_LOG_ENABLE | (J/N)       | Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle. |

| Parameter                     | Einstellung                | Beschreibung                                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIV_LOG_RETENTION          | Anzahl_der_Tage            | Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden.<br><br>Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein.                                                                                              |
| ARCHIVE_LOG_DIR               | change_info_directory/logs | Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.                                                                                                                                                                                           |
| ARCHIVE_LOG_EXT               | Dateierweiterung           | Gibt die Erweiterungslänge der Archivprotokolldatei an.<br><br>Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.161518551942 9 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (J/N)                      | Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen.<br><br>Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.                                                                        |



Die benutzerdefinierten Schlüssel-Wert-Paare werden für SAP HANA Linux-Plug-In-Systeme unterstützt und nicht für SAP HANA-Datenbanken, die als zentrales Windows-Plug-In registriert sind.

- c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                                                                        | Dann...                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar. | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.<br><br>Diese Option ist für das SnapCenter -Plug-in für die SAP HANA-Datenbank nicht anwendbar. |

| Falls Sie es wollen...                                                                              | Dann...                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                          | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                                                                     |
| Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot-Kopien zu erstellen. | Wählen Sie <b>Andere</b> aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen. |

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

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



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

Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

- b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \*  \* für die Richtlinie, die Sie konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist „policy\_name“ 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. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für SAP HANA-Ressourcen 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                  |
|------------------------------------------------------|----------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> . |



| Wenn Sie wollen...          | Machen Sie Folgendes...                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Planen Sie eine Überprüfung | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für die SAP HANA-Datenbank

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern, Wiederherstellen oder Klonen von SAP HANA-Datenbanken verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

### Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mithilfe des Cmdlets „Open-SmConnection“.

```
PS C:\> Open-SmStorageConnection
```

2. Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

Dieses Beispiel zeigt, wie Sie mit Windows-Anmeldeinformationen neue Anmeldeinformationen mit dem Namen „FinanceAdmin“ erstellen:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. Fügen Sie den SAP HANA-Kommunikationshost zum SnapCenter Server hinzu.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode hana
```

5. Installieren Sie das Paket und das SnapCenter -Plug-in für die SAP HANA-Datenbank auf dem Host.

Für Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
hana
```

Für Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana  
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. Legen Sie den Pfad zum HDBSQL-Client fest.

Für Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
hana -configSettings @{ "HANA_HDBSQL_CMD" = "C:\Program  
Files\sap\hdbclient\hdbsql.exe" }
```

Für Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com  
-PluginCode hana -configSettings  
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

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"](#) .

## Sichern Sie SAP HANA-Datenbanken

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Stellen Sie bei Sicherungsvorgängen auf Basis von Snapshot-Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Um Backups der SAP HANA-Systemreplikation zu erstellen, wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. Dadurch wird eine nahtlose Sicherung während des Übernahme-Failback-Modus gewährleistet.

["Erstellen von Ressourcengruppen und Anfügen von Richtlinien"](#) .

["Sichern von Ressourcengruppen"](#)

- Wenn Sie eine dateibasierte Sicherung erstellen möchten, wenn eine oder mehrere Mandantendatenbanken ausgefallen sind, setzen Sie den Parameter `ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT` in der HANA-Eigenschaftendatei auf **YES**. Verwenden Sie dazu `Set-SmConfigSettings` Cmdlet.

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"](#)

- Bei Pre- und Post-Befehlen für Quiesce-, Snapshot- und Unquiesce-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: `C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
  - Standardspeicherort auf dem Linux-Host: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Wählen \*\* und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- Wählen Sie den Pfeil **Backups** aus, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                            | Machen Sie Folgendes...                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Vorgangs „Consistency Group Snapshot“ zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für die Fertigstellung des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                           | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

- Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.

Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

- Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                   | Dann...                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                               | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                      |
| SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.                                       |
| So geben Sie den Befehl zum Erstellen eines Snapshots ein                                                                                                | Wählen Sie <b>Andere</b> und geben Sie dann den Befehl zum Erstellen eines Snapshots ein. |

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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

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

- b. Wählen \* \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

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

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Wählen Sie **Jetzt sichern**.

10. 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. Wählen Sie **Backup**.

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

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl.

Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript startet der Befehl `do_start method` den SnapCenter VMware-Plug-in-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Fügen Sie Ressourcen mithilfe des Cmdlets `Add-SmResources` hinzu.

Dieses Beispiel zeigt, wie Sie eine SAP HANA-Datenbank vom Typ „SingleContainer“ hinzufügen:

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary
"}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

Dieses Beispiel zeigt, wie Sie eine SAP HANA-Datenbank vom Typ „MultipleContainers“ hinzufügen:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

Dieses Beispiel zeigt, wie eine Nicht-Datenvolumenressource erstellt wird:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

### 3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

In diesem Beispiel wird eine Sicherungsrichtlinie für eine auf Snapshot-Kopien basierende Sicherung erstellt:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

In diesem Beispiel wird eine Sicherungsrichtlinie für eine dateibasierte Sicherung erstellt:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

### 4. Schützen Sie die Ressource oder fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

Dieses Beispiel schützt eine einzelne Containerressource:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Dieses Beispiel schützt eine Ressource mit mehreren Containern:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

In diesem Beispiel wird eine neue Ressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sscore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sscore.test.com";"Uid"="MDC\SID"})
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

In diesem Beispiel wird eine Ressourcengruppe ohne Datenvolume erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

##### 5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert wird:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```



In diesem Beispiel wird eine geschützte Ressource gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Überwachen Sie den Auftragsstatus (wird ausgeführt, abgeschlossen oder fehlgeschlagen) mithilfe des Cmdlets `Get-smJobSummaryReport`.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Überwachen Sie die Details des Sicherungsauftrags wie Sicherungs-ID und Sicherungsname, um mithilfe des Cmdlets `Get-SmBackupReport` Wiederherstellungs- oder Klonvorgänge durchzuführen.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId               : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime              : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

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"](#) .

## Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

### Informationen zu diesem Vorgang

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie  und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
  - a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Überwachen Sie Sicherungsvorgänge für SAP HANA-Datenbanken

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 für SAP HANA-Datenbanken 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.

## Abbrechen von Sicherungsvorgängen für SAP HANA

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzuberechnen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li><li>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                          |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>b. Wählen Sie den Vorgang aus.</li><li>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li></ol> |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## Anzeigen von SAP HANA-Datenbanksicherungen und -klonen auf der Seite „Topologie“

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

### Informationen zu diesem Vorgang

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.

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

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 **Zusammenfassungskarte**, um eine Zusammenfassung der Anzahl der auf dem

primären und sekundären Speicher verfügbaren Backups und Klone anzuzeigen.

Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der dateibasierten Sicherungen, auf Snapshot-Kopien basierenden Sicherungen und Klone an.

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 die Anwendungsressource auf 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.

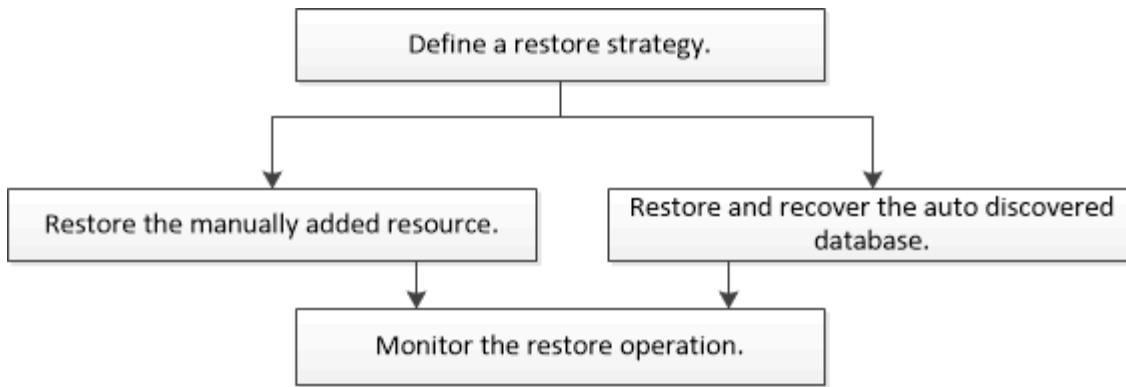
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf  .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf  .

## Wiederherstellen von SAP HANA-Datenbanken

### Wiederherstellungs-Workflow

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Wiederherstellen und Wiederherstellen einer manuell hinzugefügten Ressourcensicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Dateibasierte Sicherungskopien können nicht aus SnapCenter wiederhergestellt werden.
- Nach dem Upgrade auf SnapCenter 4.3 können die in SnapCenter 4.2 erstellten Sicherungen wiederhergestellt, jedoch nicht wiederhergestellt werden. Sie müssen HANA Studio oder externe HANA-Wiederherstellungsskripte von SnapCenter verwenden, um die in SnapCenter 4.2 erstellten Sicherungen wiederherzustellen.
- 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.
- Für den Wiederherstellungsvorgang mit SnapMirror Active Sync müssen Sie die Sicherung vom primären Speicherort auswählen.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                           |                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| search                                      |                        |
| Backup Name                                 | End Date                                                                                                  |
| rg1_scpr0191685001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ entweder **Vollständige Ressource** oder **Dateiebene** aus.

- a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumes der SAP HANA-Datenbank wiederhergestellt.

Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

- b. Wenn Sie **Dateiebene** auswählen, können Sie entweder **Alle** auswählen oder die spezifischen Volumes oder Qtrees auswählen und dann den Pfad zu diesen Volumes oder Qtrees eingeben, getrennt durch Kommas

- Sie können mehrere Volumes und Qtrees auswählen.



- Wenn der Ressourcentyp LUN ist, wird die gesamte LUN wiederhergestellt.

Sie können mehrere LUNs auswählen.



Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, Qtrees oder LUNs wiederhergestellt.

7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Befehle zum Aufheben der Bereitstellung verfügbar.

8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle verfügbar.

9. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

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

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime           | BackupType  |
|----------|-------------------------------|----------------------|-------------|
| -----    | -----                         | -----                | -----       |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:02:32 AM | Full Backup |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:23:17 AM |             |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

SmBackupId : 113  
SmJobId : 2032  
StartDateTime : 2/2/2015 6:57:03 AM  
EndDateTime : 2/2/2015 6:57:11 AM  
Duration : 00:00:07.3060000  
CreatedDateTime : 2/2/2015 6:57:23 AM  
Status : Completed  
ProtectionGroupName : Clone  
SmProtectionGroupId : 34  
PolicyName : Vault  
SmPolicyId : 18  
BackupName : Clone\_SCSPR0019366001\_02-02-2015\_06.57.08  
VerificationStatus : NotVerified

SmBackupId : 114  
SmJobId : 2183  
StartDateTime : 2/2/2015 1:02:41 PM  
EndDateTime : 2/2/2015 1:02:38 PM  
Duration : -00:00:03.2300000  
CreatedDateTime : 2/2/2015 1:02:53 PM  
Status : Completed  
ProtectionGroupName : Clone  
SmProtectionGroupId : 34  
PolicyName : Vault  
SmPolicyId : 18  
BackupName : Clone\_SCSPR0019366001\_02-02-2015\_13.02.45  
VerificationStatus : NotVerified

### 3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId  
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269  
-Confirm:$false  
output:  
Name : Restore  
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'  
Id : 2368  
StartTime : 10/4/2016 11:22:02 PM  
EndTime :  
IsCancellable : False  
IsRestartable : False  
IsCompleted : False  
IsVisible : True  
IsScheduled : False  
PercentageCompleted : 0  
Description :  
Status : Queued  
Owner :  
Error :  
Priority : None  
Tasks : {}  
ParentJobID : 0  
EventId : 0  
JobTypeId :  
ApisJobKey :  
ObjectId : 0  
PluginCode : NONE  
PluginName :
```

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"](#) .

## Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.

- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: `C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
  - Standardspeicherort auf dem Linux-Host: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Dateibasierte Sicherungskopien können nicht aus SnapCenter wiederhergestellt werden.
- Nach dem Upgrade auf SnapCenter 4.3 können die in SnapCenter 4.2 erstellten Sicherungen wiederhergestellt, jedoch nicht wiederhergestellt werden. Sie müssen HANA Studio oder externe HANA-Wiederherstellungsskripte von SnapCenter verwenden, um die in SnapCenter 4.2 erstellten Sicherungen wiederherzustellen.
- Bei ONTAP 9.12.1 und früheren 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.
- 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. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                            |                     |
|----------------------------------------------|---------------------|
| search                                       |                     |
| Backup Name                                  | End Date            |
| rg1_scspr0191683001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option „Vollständige Ressource“ aus, um die konfigurierten Datenvolumes der SAP HANA-Datenbank wiederherzustellen.



Sie können entweder **Complete Resource** (mit oder ohne **Volume Revert**) oder **Tenant Database** auswählen.

Der Wiederherstellungsvorgang wird vom SnapCenter Server für mehrere Mandanten nicht unterstützt, wenn der Benutzer entweder die Option **Mandantendatenbank** oder **Vollständige Wiederherstellung** auswählt. Sie müssen HANA Studio oder ein HANA-Python-Skript verwenden, um den Wiederherstellungsvorgang durchzuführen.

- a. Wählen Sie **Volume Revert**, wenn Sie das gesamte Volume wiederherstellen möchten.

Diese Option ist für Sicherungen verfügbar, die in SnapCenter 4.3 in NFS-Umgebungen erstellt wurden.

Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht. Dies ist anwendbar, wenn für die Wiederherstellung die Option **Complete Resource** mit **Volume Revert** ausgewählt ist.

- b. Wählen Sie **Mandantendatenbank** aus.

Diese Option ist nur für MDC-Ressourcen verfügbar.

Stellen Sie sicher, dass Sie die Mandantendatenbank stoppen, bevor Sie den Wiederherstellungsvorgang durchführen.

Wenn Sie die Option **Mandantendatenbank** auswählen, müssen Sie HANA Studio oder externe HANA-Wiederherstellungsskripts von SnapCenter verwenden, um den Wiederherstellungsvorgang durchzuführen.

7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:

| Wenn du...                                                              | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Möchten Sie so nah wie möglich an die aktuelle Zeit zurückkehren</p> | <p>Wählen Sie <b>Auf den letzten Zustand wiederherstellen</b>. Geben Sie für einzelne Containerressourcen einen oder mehrere Protokoll- und Katalogsicherungsspeicherorte an.</p> <p>Geben Sie für Multitenant-Datenbankcontainer-Ressourcen (MDC) einen oder mehrere Protokollsicherungsspeicherorte und den Speicherort des Sicherungskatalogs an.</p> <p>Bei MDC-Ressourcen sollte der Pfad sowohl Systemdatenbank- als auch Mandantendatenbankprotokolle enthalten.</p> |

| Wenn du...                                                        | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Möchten Sie den angegebenen Zeitpunkt wiederherstellen</p>     | <p>Wählen Sie <b>Zu einem bestimmten Zeitpunkt wiederherstellen</b>.</p> <p>a. Wählen Sie die Zeitzone aus.</p> <p>Die Zeitzone des Browsers ist standardmäßig ausgefüllt.</p> <p>Die ausgewählte Zeitzone wird zusammen mit der eingegebenen Zeit in absolute GMT umgerechnet.</p> <p>b. Geben Sie Datum und Uhrzeit ein.</p> <p>Beispielsweise befindet sich der HANA Linux-Host in Sunnyvale, Kalifornien, und der Benutzer in Raleigh, North Carolina, stellt die Protokolle in SnapCenter wieder her.</p> <p>Der Zeitunterschied zwischen diesen beiden Standorten beträgt 3 Stunden und da sich der Benutzer von Raleigh, NC aus angemeldet hat, ist die in der GUI ausgewählte Standardzeitzone des Browsers GMT-04:00.</p> <p>Wenn der Benutzer eine Wiederherstellung auf 5 Uhr morgens in Sunnyvale, CA durchführen möchte, muss er die Zeitzone des Browsers auf die Zeitzone des HANA Linux-Hosts (GMT-07:00) einstellen und Datum und Uhrzeit als 5:00 Uhr morgens angeben.</p> <p>Geben Sie für einzelne Containerressourcen einen oder mehrere Protokoll- und Katalogsicherungsspeicherorte an.</p> <p>Geben Sie für MDC-Ressourcen einen oder mehrere Protokollsicherungsspeicherorte und den Speicherort des Sicherungskatalogs an.</p> <p>Bei MDC-Ressourcen sollte der Pfad sowohl Systemdatenbank- als auch Mandantendatenbankprotokolle enthalten.</p> |
| <p>Möchten Sie eine bestimmte Datensicherung wiederherstellen</p> | <p>Wählen Sie <b>Aus angegebener Datensicherung wiederherstellen</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>Will nicht erholen</p>                                         | <p>Wählen Sie <b>Keine Wiederherstellung</b>. Sie müssen den Wiederherstellungsvorgang manuell vom HANA-Studio aus durchführen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Sie können nur die Sicherungen wiederherstellen, die nach dem Upgrade auf SnapCenter 4.3 erstellt

wurden, vorausgesetzt, sowohl der Host als auch das Plug-In werden auf SnapCenter 4.3 aktualisiert und die zur Wiederherstellung ausgewählten Sicherungen werden erstellt, nachdem die Ressource konvertiert oder als automatisch erkannte Ressource erkannt wurde.

8. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Befehle zum Aufheben der Bereitstellung verfügbar.

9. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle verfügbar.

10. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets

Das Wiederherstellen einer Ressourcensicherung umfasst das Einleiten einer Verbindungssitzung mit dem SnapCenter -Server, das Auflisten der Sicherungen und Abrufen von Sicherungsinformationen sowie das Wiederherstellen einer Sicherung.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „`Get-SmBackup`“ und „`Get-SmBackupReport`“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:



```
PS C:\> Get-SmBackup
```

| BackupId    | BackupName                             | BackupTime  |
|-------------|----------------------------------------|-------------|
| BackupType  |                                        |             |
| -----       | -----                                  | -----       |
| -----       |                                        |             |
| 1           | Payroll Dataset_vise-f6_08... 8/4/2015 | 11:02:32 AM |
| Full Backup |                                        |             |
| 2           | Payroll Dataset_vise-f6_08... 8/4/2015 | 11:23:17 AM |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime  
"2/3/2015"
```

```
SmBackupId      : 113  
SmJobId         : 2032  
StartDateTime   : 2/2/2015 6:57:03 AM  
EndDateTime     : 2/2/2015 6:57:11 AM  
Duration        : 00:00:07.3060000  
CreatedDateTime : 2/2/2015 6:57:23 AM  
Status          : Completed  
ProtectionGroupName : Clone  
SmProtectionGroupId : 34  
PolicyName      : Vault  
SmPolicyId      : 18  
BackupName      : Clone_SCSPR0019366001_02-02-2015_06.57.08  
VerificationStatus : NotVerified
```

```
SmBackupId      : 114  
SmJobId         : 2183  
StartDateTime   : 2/2/2015 1:02:41 PM  
EndDateTime     : 2/2/2015 1:02:38 PM  
Duration        : -00:00:03.2300000  
CreatedDateTime : 2/2/2015 1:02:53 PM  
Status          : Completed  
ProtectionGroupName : Clone  
SmProtectionGroupId : 34  
PolicyName      : Vault  
SmPolicyId      : 18  
BackupName      : Clone_SCSPR0019366001_02-02-2015_13.02.45  
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :

```

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"](#).

## Überwachen von Wiederherstellungsvorgängen für SAP HANA-Datenbanken

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 von SAP HANA-Ressourcensicherungen

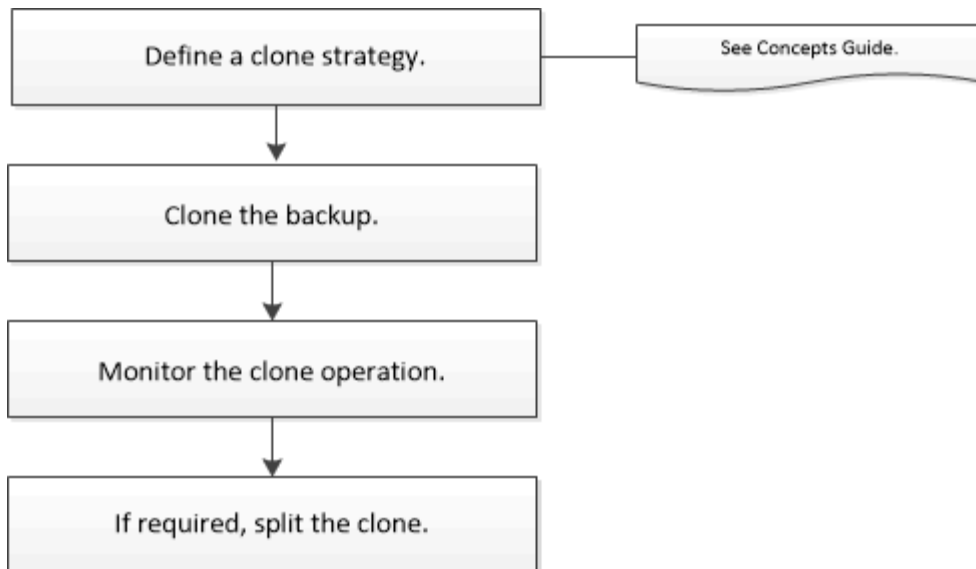
### Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

#### Informationen zu diesem Vorgang

- Sie können auf dem SAP HANA-Quellserver klonen.
- Sie können Ressourcensicherungen aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Für Datenextraktions- und Manipulationstools beim Befüllen von Data Warehouses
  - So stellen Sie versehentlich gelöschte oder geänderte Daten wieder her

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

## Klonen einer SAP HANA-Datenbanksicherung

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen.

### Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Sie können keine dateibasierten Sicherungen klonen.
- Der Zielklonserver sollte dieselbe SID der SAP HANA-Instanz haben, die im Feld „Zielklon-SID“ angegeben ist.
- Bei Befehlen vor oder nach dem Klonen sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Für Windows: `C:\Programme\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
  - Für Linux: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Informationen zu den Einschränkungen beim Klon-Split-Vorgang finden Sie unter "[ONTAP 9 Handbuch zur logischen Speicherverwaltung](#)".
- Bei ONTAP 9.12.1 und früheren 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:

| Für dieses Feld...    | Machen Sie Folgendes...                                                                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plug-in-Host          | Wählen Sie den Host aus, auf dem der Klon gemountet werden soll und das Plug-In wird installiert.                                                                      |
| Zielklon-SID          | Geben Sie die ID der SAP HANA-Instanz ein, die aus den vorhandenen Sicherungen geklont werden soll.                                                                    |
| NFS-Export-IP-Adresse | Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden.                                                                         |
| iSCSI-Initiator       | Geben Sie den iSCSI-Initiatornamen des Hosts ein, auf den die LUNs exportiert werden. Diese Option ist nur verfügbar, wenn Sie den LUN-Ressourcentyp ausgewählt haben. |
| Protokoll             | Geben Sie das LUN-Protokoll ein. Diese Option ist nur verfügbar, wenn Sie den LUN-Ressourcentyp ausgewählt haben.                                                      |

Wenn es sich bei der ausgewählten Ressource um eine LUN handelt und Sie von einer sekundären Sicherung klonen, werden die Zielvolumes aufgelistet. Eine einzelne Quelle kann mehrere Zielvolumes haben.



Vor dem Klonen müssen Sie sicherstellen, dass der iSCSI-Initiator oder der FCP vorhanden und bei alternativen Hosts konfiguriert und angemeldet ist.

7. Führen Sie auf der Seite „Skripts“ die folgenden Schritte aus:



Die Skripte werden auf dem Plug-in-Host ausgeführt.

- a. Geben Sie die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
  - Befehl vor dem Klonen: Löschen Sie vorhandene Datenbanken mit demselben Namen
  - Befehl nach dem Klonen: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.
- b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Mount-Befehl für ein Volume oder einen Qtree auf einer Linux-Maschine:

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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.

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

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

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146/
```

2. Rufen Sie die Sicherungen ab, um den Klonvorgang mithilfe des Cmdlets „`Get-SmBackup`“ durchzuführen.

Dieses Beispiel zeigt, dass zwei Sicherungen zum Klonen verfügbar sind:

```
C:\PS> Get-SmBackup
```

| BackupId             | BackupName                    |
|----------------------|-------------------------------|
| BackupTime           | BackupType                    |
| -----                | -----                         |
| 1                    | Payroll Dataset_vise-f6_08... |
| 8/4/2015 11:02:32 AM | Full Backup                   |
| 2                    | Payroll Dataset_vise-f6_08... |
| 8/4/2015 11:23:17 AM |                               |

3. Starten Sie einen Klonvorgang von einer vorhandenen Sicherung und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

Dieses Beispiel zeigt, dass das zu klonende Backup eine NFSExportIPs-Adresse von 10.232.206.169 hat:

```
New-SmClone -AppPluginCode hana -BackupName  
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-  
2017_02.54.29.3817 -Resources  
@{"Host"="scsccore1.sccore.test.com";"Uid"="H73"} -CloneToInstance  
shivscc4.sccore.test.com -mountcommand 'mount  
10.232.206.169:%hana73data_Clone /hana83data'  
-preclonecreatecommands '/home/scripts/scpre_clone.sh'  
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```



Wenn NFSExportIPs nicht angegeben ist, wird der Standardwert auf den Klonzielhost exportiert.

4. Überprüfen Sie, ob die Sicherungen erfolgreich geklont wurden, indem Sie mit dem Cmdlet „Get-SmCloneReport“ die Details des Klonauftrags anzeigen.

Sie können Details wie Klon-ID, Startdatum und -uhrzeit sowie Enddatum und -uhrzeit anzeigen.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId             : 186
StartDateTime       : 8/3/2015 2:43:02 PM
EndDateTime        : 8/3/2015 2:44:08 PM
Duration            : 00:01:06.6760000
Status              : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName          : OnDemand_Clone
SmPolicyId          : 4
BackupPolicyName    : OnDemand_Full_Log
SmBackupPolicyId    : 1
CloneHostName      : SCSPR0054212005.mycompany.com
CloneHostId        : 4
CloneName           : Draper__clone__08-03-2015_14.43.53
SourceResources     : {Don, Betty, Bobby, Sally}
ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError          :
```

## Überwachen von SAP HANA-Datenbankklonvorgängen

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**.

## 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 <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme         | Wählen Sie <b>Pfad</b> 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"](#)

## Löschen oder Aufteilen von SAP HANA-Datenbankklonen nach dem Upgrade von SnapCenter

Nach dem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource aufteilen, aus der die Klone erstellt wurden.

### Informationen zu diesem Vorgang

Wenn Sie den Speicherbedarf der versteckten Klone ermitteln möchten, führen Sie den folgenden Befehl aus:  
`Get-SmClone -ListStorageFootprint`

### Schritte

1. Löschen Sie die Sicherungen der geklonten Ressourcen mithilfe des Cmdlets „remove-smbbackup“.
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mithilfe des Cmdlets „remove-smresourcegroup“.
3. Entfernen Sie den Schutz der geklonten Ressource mithilfe des Cmdlets „remove-smprotectresource“.
4. Wählen Sie die übergeordnete Ressource auf der Seite „Ressourcen“ aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht „Kopien verwalten“ die Klone entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
6. Wählen Sie die Klone aus und klicken Sie dann auf  , um Klone zu löschen, oder klicken Sie auf  um die Klone zu teilen.

7. Klicken Sie auf **OK**.

# Schützen Sie Oracle-Datenbanken

## Übersicht über das SnapCenter -Plug-in für Oracle-Datenbanken

### Was können Sie mit dem Plug-in für Oracle Database tun?

Das SnapCenter -Plug-in für Oracle-Datenbanken ist eine hostseitige Komponente der NetApp SnapCenter -Software, die eine anwendungsbewusste Datenschutzverwaltung von Oracle-Datenbanken ermöglicht.

Das Plug-in für Oracle Database automatisiert die Sicherung, Katalogisierung und Dekatalogisierung mit Oracle Recovery Manager (RMAN), die Überprüfung, das Mounten, Unmounten, Wiederherstellen, Recovery und Klonen von Oracle-Datenbanken in Ihrer SnapCenter Umgebung. Das Plug-in für Oracle-Datenbanken installiert das SnapCenter Plug-in für UNIX, um alle Datenschutzvorgänge durchzuführen.

Mit dem Plug-in für Oracle-Datenbanken können Sie Sicherungen von Oracle-Datenbanken verwalten, auf denen SAP-Anwendungen ausgeführt werden. Die SAP BR\*Tools-Integration wird jedoch nicht unterstützt.

- Sichern Sie Datendateien, Steuerdateien und archivieren Sie Protokolldateien.

Die Sicherung wird nur auf Containerdatenbankebene (CDB) unterstützt.

- Wiederherstellung und Wiedergewinnung von Datenbanken, CDBs und Pluggable Databases (PDBs).

Unvollständige Wiederherstellungen von PDBs werden nicht unterstützt.

- Erstellen Sie Klone von Produktionsdatenbanken bis zu einem bestimmten Zeitpunkt.

Das Klonen wird nur auf CDB-Ebene unterstützt.

- Überprüfen Sie die Sicherungen sofort.
- Mounten und Unmounten von Daten und Protokollsicherungen für den Wiederherstellungsvorgang.
- Planen Sie Sicherungs- und Überprüfungsvorgänge.
- Überwachen Sie alle Vorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.
- Automatisiert anwendungsorientierte Sicherungs-, Wiederherstellungs-, Überprüfungs-, Mount-, Unmount- und Klonvorgänge für Oracle-Datenbanken in Ihrer SnapCenter Umgebung
- Unterstützt Oracle-Datenbanken für SAP, jedoch ist keine SAP BR\*Tools-Integration vorgesehen

### Funktionen des Plug-ins für Oracle-Datenbanken

Das Plug-in für Oracle Database lässt sich in die Oracle-Datenbank auf dem Linux- oder AIX-Host und in NetApp -Technologien auf dem Speichersystem integrieren.

- Einheitliche grafische Benutzeroberfläche

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und

Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- Automatisierte zentrale Verwaltung

Sie können Sicherungs- und Klonvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- Unterbrechungsfreie NetApp Snapshot-Technologie

SnapCenter verwendet die NetApp Snapshot-Technologie mit dem Plug-in für Oracle-Datenbanken und dem Plug-in für UNIX zum Sichern von Datenbanken. Snapshots verbrauchen nur minimalen Speicherplatz.

Das Plug-in für Oracle Database bietet außerdem die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs-, Klon-, Mount-, Unmount- und Überprüfungs-Workflows
- Automatische Erkennung der auf dem Host konfigurierten Oracle-Datenbanken
- Unterstützung für die Katalogisierung und Dekatalogisierung mit Oracle Recovery Manager (RMAN)
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Unterstützung für Archive Log Management (ALM) für Wiederherstellungs- und Klonvorgänge
- Erstellung platzsparender und zeitpunktbezogener Kopien von Produktionsdatenbanken zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung der Consistency Group (CG)-Funktion von ONTAP als Teil der Erstellung von Backups in SAN- und ASM-Umgebungen
- Unterbrechungsfreie und automatisierte Backup-Verifizierung
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Datenbankhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Datenbanken auf einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Unterstützung für physische und virtualisierte Infrastrukturen
- Unterstützung für NFS, iSCSI, Fibre Channel (FC), RDM, VMDK über NFS und VMFS sowie ASM über NFS, SAN, RDM und VMDK
- Unterstützung für die Selective LUN Map (SLM)-Funktion von ONTAP

Die standardmäßig aktivierte SLM-Funktion erkennt regelmäßig die LUNs, die keine optimierten Pfade haben, und behebt diese. Sie können SLM konfigurieren, indem Sie die Parameter in der Datei `scu.properties` unter `/var/opt/snapcenter/scu/etc` ändern.

- Sie können dies deaktivieren, indem Sie den Wert des Parameters

ENABLE\_LUNPATH\_MONITORING auf „false“ setzen.

- Sie können die Häufigkeit angeben, mit der die LUN-Pfade automatisch repariert werden, indem Sie dem Parameter LUNPATH\_MONITORING\_INTERVAL den Wert (in Stunden) zuweisen. Informationen zu SLM finden Sie im ["ONTAP 9 SAN-Administrationsabschnitt"](#).

- Unterstützung für Non-Volatile Memory Express (NVMe) unter Linux

- NVMe Util sollte auf dem Host installiert sein.

Sie müssen das NVMe-Dienstprogramm installieren, um auf einem alternativen Host zu klonen oder zu mounten.

- Mit Ausnahme der virtualisierten Umgebungen wie RDM werden auf der NVMe-Hardware Sicherungs-, Wiederherstellungs-, Klon-, Mount-, Unmount-, Katalogisierungs-, Dekatalogisierungs- und Überprüfungsvorgänge unterstützt.

Die oben genannten Vorgänge werden auf Geräten ohne Partitionen oder mit einer einzelnen Partition unterstützt.



Sie können eine Multipathing-Lösung für NVMe-Geräte konfigurieren, indem Sie die native Multipathing-Option im Kernel festlegen. Device Mapper (DM)-Multipathing wird nicht unterstützt.

- Die Workflows „Sicherungs-, Wiederherstellungs-, Klon-, Mount-, Unmount-, Katalogisierungs-, Dekatalogisierungs- und Überprüfungs-Workflows“ werden auf NVMe über TCP/IP unterstützt.
- Die Arbeitsabläufe zum Sichern, Wiederherstellen, Klonen, Einbinden, Ausbinden, Katalogisieren, Entkatalogisieren und Überprüfen werden auf einem VMDK-Layout unterstützt, das auf NVMe über TCP/IP erstellt wurde.

- Unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie transparent ausfallen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.
- Unterstützt jeden nicht standardmäßigen Benutzer anstelle von Oracle und Grid.

Um die nicht standardmäßigen Benutzer zu unterstützen, sollten Sie die nicht standardmäßigen Benutzer festlegen, indem Sie die Werte der Parameter in der Datei **sco.properties** unter *file* `/var/opt/snapcenter/sco/etc/` ändern.

Die Standardwerte der Parameter sind auf Oracle und Grid festgelegt.

- DB\_USER=Oracle
- DB\_GROUP=oinstall
- GI\_USER=Raster
- GI\_GROUP=oinstall

## Vom Plug-in für Oracle-Datenbank unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen auf physischen und virtuellen Maschinen. Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket

für AIX installieren.

SnapCenter unterstützt keine Speicherbereitstellung für Linux und AIX.

### Unter Linux unterstützte Speichertypen

In der folgenden Tabelle sind die unter Linux unterstützten Speichertypen aufgeführt.

| Maschine          | Speichertyp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | <ul style="list-style-type: none"><li>• FC-verbundene LUNs</li><li>• Über iSCSI verbundene LUNs</li><li>• Über NFS verbundene Volumes</li><li>• NVMe-FC</li><li>• NVMe/TCP</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| VMware ESXi       | <ul style="list-style-type: none"><li>• RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt.<br/><br/>Sie können die Datei <b>LinuxConfig.pm</b> unter <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> bearbeiten, um den Wert des Parameters <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> auf 1 zu setzen und nur die HBAs erneut zu scannen, die in <code>HBA_DRIVER_NAMES</code> aufgeführt sind.</li><li>• iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind</li><li>• VMDKs auf NFS-Datenspeichern</li><li>• VMDKs auf VMFS, die über NVMe/TCP erstellt wurden</li></ul> <div><p>RAC wird auf ESX 8.0U2 unterstützt, das die Unterstützung für gemeinsam genutzte VMDK bietet</p></div> <ul style="list-style-type: none"><li>• NFS-Volumes, die direkt mit dem Gastsystem verbunden sind</li><li>• vVol-Datenspeicher auf NFS und SAN</li></ul> <p>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p> |

## Unter AIX unterstützte Speichertypen

In der folgenden Tabelle sind die unter AIX unterstützten Speichertypen aufgeführt.

| Maschine          | Speichertyp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | <ul style="list-style-type: none"><li>• FC-verbundene und iSCSI-verbundene LUNs.</li></ul> <p>In einer SAN-Umgebung werden ASM-, LVM- und SAN-Dateisysteme unterstützt.</p> <div> NFS auf AIX und Dateisystem wird nicht unterstützt.</div> <ul style="list-style-type: none"><li>• Erweitertes Journaled File System (JFS2)</li></ul> <p>Unterstützt Inline-Protokollierung auf SAN-Dateisystemen und LVM-Layout.</p> |

Der "[NetApp Interoperabilitätsmatrix-Tool](#)" enthält die neuesten Informationen zu den unterstützten Versionen.

## Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für Plug-in für Oracle vor

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im "[ONTAP-Dokumentation](#)".



## Für das Plug-in für Oracle sind mindestens ONTAP -Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

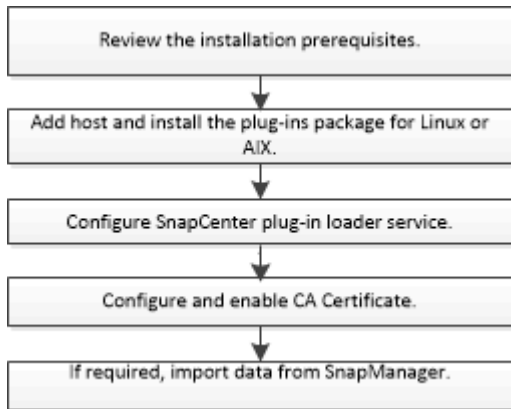
- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN-Attribut anzeigen
  - LUN erstellen
  - LUN löschen
  - LUN-Geometrie
  - lun igroup hinzufügen
  - lun igroup erstellen
  - LUN-Igroup löschen
  - LUN-Igroup umbenennen
  - lun igroup show
  - LUN-Zuordnung Add-Reporting-Nodes
  - LUN-Zuordnung erstellen
  - LUN-Zuordnung löschen
  - LUN-Zuordnung zum Entfernen von Berichtsknoten
  - LUN-Mapping-Show
  - LUN ändern
  - LUN-Einzugsvolumen
  - lun offline
  - lun online
  - LUN persistent-reservation clear
  - LUN-Größe ändern
  - LUN-Seriennummer
  - Lun-Show
  - Snapmirror-Richtlinie Add-Rule
  - Snapmirror-Richtlinienänderungsregel
  - Snapmirror-Richtlinie zum Entfernen der Regel
  - Snapmirror-Richtlinien-Show
  - Snapmirror-Wiederherstellung
  - Snapmirror-Show

- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- vServer
- VServer-CIFS
- vServer CIFS Shadowcopy anzeigen
- vServer anzeigen
- Netzwerkschnittstelle
- Netzwerkschnittstelle anzeigen
- Metrocluster-Show

# Installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank

## Installationsworkflow des SnapCenter Plug-ins für Oracle-Datenbanken

Sie sollten das SnapCenter -Plug-in für Oracle Database installieren und einrichten, wenn Sie Oracle-Datenbanken schützen möchten.



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

Bevor Sie einen Host hinzufügen und die Plug-In-Pakete installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.

Das SnapCenter Plug-in für Oracle Database 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.

- Wenn Sie das SnapCenter Plug-ins-Paket für AIX auf einem AIX-Host installieren, sollten Sie die symbolischen Links auf Verzeichnisebene manuell aufgelöst haben.

Das SnapCenter Plug-ins-Paket für AIX löst automatisch den symbolischen Link auf Dateiebene auf, nicht jedoch die symbolischen Links auf Verzeichnisebene, um den absoluten Pfad JAVA\_HOME zu erhalten.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus „Linux“ oder „AIX“ für den Installationsbenutzer.
- Sie müssen Java 11 auf Ihrem Linux- oder AIX-Host installiert haben.
  - Java von Oracle und OpenJDK wird für Linux unterstützt
  - IBM Java für AIX. Sie können von herunterladen "[IBM Semeru Runtimes-Downloads](#)"



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

- Für Oracle-Datenbanken, die auf einem Linux- oder AIX-Host ausgeführt werden, sollten Sie sowohl das SnapCenter -Plug-in für Oracle-Datenbanken als auch das SnapCenter -Plug-in für UNIX installieren.



Mit dem Plug-in für Oracle-Datenbanken können Sie auch Oracle-Datenbanken für SAP verwalten. Die SAP BR\*Tools-Integration wird jedoch nicht unterstützt.

- Wenn Sie die Oracle-Datenbank 11.2.0.3 oder höher verwenden, müssen Sie den Oracle-Patch 13366202 installieren.



Die UUID-Zuordnung in der Datei /etc/fstab wird von SnapCenter nicht unterstützt.

- 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                                                                              | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• Oracle Linux</li> </ul> <div> <p>Wenn Sie eine Oracle-Datenbank auf LVM in den Betriebssystemen Oracle Linux oder Red Hat Enterprise Linux 6.6 oder 7.0 verwenden, müssen Sie die neueste Version von Logical Volume Manager (LVM) installieren.</p> </div> <ul style="list-style-type: none"> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> |
| 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 <div> <p>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.</p> </div>                       |

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

Die neuesten Informationen zu unterstützten Versionen finden Sie im "[NetApp Interoperabilitätsmatrix-Tool](#)".

#### Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host

SnapCenter 2.0 und spätere Versionen ermöglichen es einem Nicht-Root-Benutzer, das SnapCenter -Plug-In -Paket für Linux zu installieren und den Plug-In-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

#### Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- /home/*LINUX\_USER*/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/bin/spl

## Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „/`<crs_home>/bin/olsnodes`“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`LINUX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den Prüfsummenwert aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## AIX-Hostanforderungen

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



Das SnapCenter -Plug-in für UNIX, das Teil des SnapCenter Plug-in-Pakets für AIX ist, unterstützt keine gleichzeitigen Volume-Gruppen.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | AIX 7.1 oder höher                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 4 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | 2 GB <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | Java 11 IBM Java <p>Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option <code>JAVA_HOME</code> unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.</p>                                                                                                                                                                                                       |

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#).

#### Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host

SnapCenter 4.4 und höher ermöglicht es einem Nicht-Root-Benutzer, das SnapCenter Plug-ins-Paket für AIX zu installieren und den Plug-in-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

#### Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:



```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- /home/AIX\_USER/.sc\_netapp/snapcenter\_aix\_host\_plugin.bsx
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/bin/spl

## Schritte

1. Melden Sie sich beim AIX-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für AIX installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „/`<crs_home>/bin/olsnodes`“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`AIX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Einrichten von Anmeldeinformationen

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation des Plug-In-Pakets auf Linux- oder AIX-Hosts erstellen.

### Über diese Aufgabe

Die Anmeldeinformationen werden entweder für den Root-Benutzer oder für einen Nicht-Root-Benutzer erstellt, der über Sudo-Berechtigungen zum Installieren und Starten des Plug-In-Prozesses verfügt.

Weitere Informationen finden Sie unter: [Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host](#) oder [Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host](#)

**Best Practice:** Obwohl Sie Anmeldeinformationen nach der Bereitstellung von Hosts und der Installation von Plug-Ins erstellen dürfen, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die Anmeldeinformationen ein:

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |

| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername/Passwort             | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator</li> </ul> <p>Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> </ul> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i></p> |
| Authentifizierungsmodus           | <p>Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.</p> <p>Wählen Sie je nach Betriebssystem des Plug-in-Hosts entweder Linux oder AIX aus.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen <b>Sudo-Berechtigungen verwenden</b>, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite **Benutzer und Zugriff** zuweisen.

### Konfigurieren der Anmeldeinformationen für eine Oracle-Datenbank

Sie müssen Anmeldeinformationen konfigurieren, die zum Ausführen von Datenschutzvorgängen in Oracle-Datenbanken verwendet werden.

### Über diese Aufgabe

Sie sollten die verschiedenen für die Oracle-Datenbank unterstützten Authentifizierungsmethoden überprüfen. Weitere Informationen finden Sie unter "[Authentifizierungsmethoden für Ihre Anmeldeinformationen](#)".

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, muss der Benutzername mindestens über Ressourcengruppen- und Sicherungsrechte verfügen.

Wenn Sie die Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ressourcenansicht ein rotes Vorhängeschlosssymbol angezeigt. Sie müssen Datenbankanmeldeinformationen konfigurieren, um die Datenbank schützen zu können, oder sie der Ressourcengruppe hinzufügen, um Datenschutzvorgänge durchzuführen.



Wenn Sie beim Erstellen eines Berechtigungsnachweises falsche Angaben machen, wird eine Fehlermeldung angezeigt. Sie müssen auf **Abbrechen** klicken und es dann erneut versuchen.

## 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 „Datenbank“ aus.
3. Klicken  und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern.

Sie können dann auf , um den Filterbereich zu schließen.

4. Wählen Sie die Datenbank aus und klicken Sie dann auf **Datenbankeinstellungen > Datenbank konfigurieren**.
5. Wählen Sie im Abschnitt „Datenbankeinstellungen konfigurieren“ aus der Dropdownliste **Vorhandene Anmeldeinformationen verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datenschutzjobs in der Oracle-Datenbank verwendet werden sollen.



Der Oracle-Benutzer sollte über Sysdba-Berechtigungen verfügen.

Sie können auch Anmeldeinformationen erstellen, indem Sie auf .

6. Wählen Sie im Abschnitt „ASM-Einstellungen konfigurieren“ aus der Dropdownliste **Vorhandene Anmeldeinformationen verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datenschutzjobs auf der ASM-Instanz verwendet werden sollen.



Der ASM-Benutzer sollte über Sysasm-Berechtigungen verfügen.

Sie können auch Anmeldeinformationen erstellen, indem Sie auf .

7. Wählen Sie im Abschnitt „RMAN-Katalogeinstellungen konfigurieren“ aus der Dropdownliste **Vorhandene Anmeldeinformationen verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datenschutzjobs in der Oracle Recovery Manager (RMAN)-Katalogdatenbank verwendet werden sollen.

Sie können auch Anmeldeinformationen erstellen, indem Sie auf .

Geben Sie im Feld **TNSName** den Dateinamen des Transparent Network Substrate (TNS) ein, der vom SnapCenter -Server zur Kommunikation mit der Datenbank verwendet wird.

8. Geben Sie im Feld **Bevorzugte RAC-Knoten** die für die Sicherung bevorzugten Real Application Cluster

(RAC)-Knoten an.

Bei den bevorzugten Knoten kann es sich um einen oder alle Clusterknoten handeln, auf denen die RAC-Datenbankinstanzen vorhanden sind. Der Sicherungsvorgang wird nur auf diesen bevorzugten Knoten in der Reihenfolge der Präferenz ausgelöst.

In RAC One Node ist nur ein Knoten in den bevorzugten Knoten aufgeführt, und dieser bevorzugte Knoten ist der Knoten, auf dem die Datenbank derzeit gehostet wird.

Nach einem Failover oder einer Verlagerung der RAC One Node-Datenbank wird durch die Aktualisierung der Ressourcen auf der SnapCenter Ressourcenseite der Host aus der Liste **Bevorzugte RAC-Knoten** entfernt, auf dem die Datenbank zuvor gehostet wurde. Der RAC-Knoten, auf den die Datenbank verschoben wird, wird in **RAC-Knoten** aufgeführt und muss manuell als bevorzugter RAC-Knoten konfiguriert werden.

Weitere Informationen finden Sie unter ["Bevorzugte Knoten im RAC-Setup"](#) .

9. Klicken Sie auf **OK**.

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

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

### Über diese Aufgabe

Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie das Plug-in auf einem Cluster (Oracle RAC) installieren, wird das Plug-in auf allen Knoten des Clusters installiert. Für Oracle RAC One Node sollten Sie das Plug-in sowohl auf aktiven als auch auf passiven Knoten installieren.



Wenn Sie das Plug-In auf einem Oracle RAC installieren, wird nur die kennwortbasierte Authentifizierung unterstützt. Die auf SSH-Schlüsseln basierende Authentifizierung wird nicht unterstützt.

Ihnen sollte eine Rolle zugewiesen werden, die über die Berechtigung zum Installieren und Deinstallieren des Plug-Ins verfügt, beispielsweise die SnapCenter Administratorrolle.



Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.

### 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              | <p>Wählen Sie <b>Linux</b> oder <b>AIX</b> als Hosttyp.</p> <p>Der SnapCenter -Server fügt den Host hinzu und installiert dann das Plug-in für Oracle Database und das Plug-in für UNIX, falls die Plug-ins nicht bereits auf dem Host installiert sind.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Hostname             | <p>Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.</p> <p>SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p> <p>Sie können die IP-Adressen oder den FQDN eines der folgenden Elemente eingeben:</p> <ul style="list-style-type: none"> <li>• Eigenständiger Host</li> <li>• Jeder Knoten in der Oracle Real Application Clusters (RAC)-Umgebung</li> </ul> <div data-bbox="922 909 976 968">  </div> <div data-bbox="1036 905 1409 968"> <p>Knoten-VIP oder Scan-IP wird nicht unterstützt</p> </div> <p>Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.</p> |
| Anmeldeinformationen | <p>Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen.</p> <p>Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen von Anmeldeinformationen.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div data-bbox="873 1759 927 1818">  </div> <div data-bbox="987 1696 1409 1871"> <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div>                                  |

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

6. (Optional) Klicken Sie auf **Weitere Optionen**.

| Für dieses Feld...                                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen                                             | <p>Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an.</p> <p>Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.</p> <div><p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p></div> |
| Installationspfad                                 | <p>Der Standardpfad ist <code>/opt/NetApp/snapcenter</code>.</p> <p>Optional können Sie den Pfad anpassen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Alle Hosts im Oracle RAC hinzufügen               | <p>Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem Oracle RAC hinzuzufügen.</p> <p>In einem Flex ASM-Setup werden alle Knoten hinzugefügt, unabhängig davon, ob es sich um einen Hub- oder Leaf-Knoten handelt.</p>                                                                                                                                                                                                                                                                                                        |
| Überspringen optionaler Vorinstallationsprüfungen | <p>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.</p>                                                                                                                                                                                                                                                                                                                                     |

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**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



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 Datenbanken auf dem Host 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**.

## Alternative Möglichkeiten zur Installation des Plug-In-Pakets für Linux oder AIX

Sie können das Plug-In-Paket für Linux oder AIX auch manuell installieren, indem Sie entweder die Cmdlets oder CLIs verwenden.

Bevor Sie das Plug-in manuell installieren, sollten Sie die Signatur des Binärpakets mithilfe der Schlüssel **snapcenter\_public\_key.pub** und **snapcenter\_linux\_host\_plugin.bin.sig** unter *C:\ProgramData\NetApp\SnapCenter\Package Repository* validieren.



Stellen Sie sicher, dass **OpenSSL 1.0.2g** auf dem Host installiert ist, auf dem Sie das Plug-in installieren möchten.

Validieren Sie die Signatur des Binärpakets, indem Sie den folgenden Befehl ausführen:

- Für Linux-Host: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Für AIX-Host: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

## Installieren Sie mithilfe von Cmdlets auf mehreren Remotehosts

Sie sollten das PowerShell-Cmdlet *Install-SmHostPackage* verwenden, um das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX auf mehreren Hosts zu installieren.

### Was Sie brauchen

Sie sollten auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet sein.

### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX mit dem Cmdlet *Install-SmHostPackage* und den erforderlichen Parametern.

Sie können die Option *-skippercheck* verwenden, 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.



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

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

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](#)

## Auf Clusterhost installieren

Sie sollten das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX auf beiden Knoten des Clusterhosts installieren.

Jeder Knoten des Cluster-Hosts hat zwei IPs. Eine der IPs ist die öffentliche IP der jeweiligen Knoten und die zweite IP ist die Cluster-IP, die von beiden Knoten gemeinsam genutzt wird.

### Schritte

1. Installieren Sie das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX auf beiden Knoten des Clusterhosts.
2. Überprüfen Sie, ob die richtigen Werte für die Parameter `SNAPCENTER_SERVER_HOST`, `SPL_PORT`, `SNAPCENTER_SERVER_PORT` und `SPL_ENABLED_PLUGINS` in der Datei `spl.properties` unter `/var/opt/snapcenter/spl/etc/` angegeben sind.

Wenn `SPL_ENABLED_PLUGINS` in `spl.properties` nicht angegeben ist, können Sie es hinzufügen und den Wert `SCO,SCU` zuweisen.

3. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
4. Legen Sie in jedem Knoten die bevorzugten IPs des Knotens mit dem `sccli`-Befehl *Set-PreferredHostIPsInStorageExportPolicy* und den erforderlichen Parametern fest.
5. Fügen Sie im SnapCenter Server-Host einen Eintrag für die Cluster-IP und den entsprechenden DNS-Namen in `C:\Windows\System32\drivers\etc\hosts` hinzu.
6. Fügen Sie den Knoten mit dem Cmdlet *Add-SmHost* zum SnapCenter -Server hinzu, indem Sie die Cluster-IP für den Hostnamen angeben.

Ermitteln Sie die Oracle-Datenbank auf Knoten 1 (vorausgesetzt, die Cluster-IP wird auf Knoten 1 gehostet) und erstellen Sie eine Sicherungskopie der Datenbank. Wenn ein Failover auftritt, können Sie die auf Knoten 1 erstellte Sicherung verwenden, um die Datenbank auf Knoten 2 wiederherzustellen. Sie können das auf Knoten 1 erstellte Backup auch verwenden, um einen Klon auf Knoten 2 zu erstellen.



Wenn das Failover erfolgt, während andere SnapCenter -Vorgänge ausgeführt werden, bleiben veraltete Volumes, Verzeichnisse und Sperrdateien übrig.

## Installieren Sie das Plug-In-Paket für Linux im unbeaufsichtigten Modus

Sie können das SnapCenter Plug-Ins-Paket für Linux im unbeaufsichtigten Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

### Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-In-Pakets überprüfen.
- Sie sollten sicherstellen, dass die Umgebungsvariable `DISPLAY` nicht festgelegt ist.

Wenn die Umgebungsvariable `DISPLAY` festgelegt ist, sollten Sie `unset DISPLAY` ausführen und dann versuchen, das Plug-In manuell zu installieren.

## Über diese Aufgabe

Bei der Installation im Konsolenmodus müssen Sie die erforderlichen Installationsinformationen angeben, bei der Installation im unbeaufsichtigten Modus hingegen müssen Sie keine Installationsinformationen angeben.

## Schritte

1. Laden Sie das SnapCenter Plug-Ins-Paket für Linux vom Installationsort des SnapCenter Servers herunter.

Der Standardinstallationspfad ist *C:\ProgramData\NetApp\ SnapCenter\PackageRepository*. Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.
3. Laufen

```
./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR=/opt/custom_path
```

4. Bearbeiten Sie die Datei *spl.properties* unter */var/opt/snapcenter/spl/etc/*, um *SPL\_ENABLED\_PLUGINS=SCO,SCU* hinzuzufügen, und starten Sie dann den Dienst SnapCenter Plug-in Loader neu.



Durch die Installation des Plug-In-Pakets werden die Plug-Ins auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie sollten die Plug-Ins auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter -GUI oder des PowerShell-Cmdlets hinzufügen. Wählen Sie beim Hinzufügen des Hosts „Keine“ als Anmeldeinformationen aus. Nachdem der Host hinzugefügt wurde, werden die installierten Plug-Ins automatisch erkannt.

## Installieren Sie das Plug-In-Paket für AIX im unbeaufsichtigten Modus

Sie können das SnapCenter Plug-ins-Paket für AIX im unbeaufsichtigten Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

### Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-In-Pakets überprüfen.
- Sie sollten sicherstellen, dass die Umgebungsvariable *DISPLAY* nicht festgelegt ist.

Wenn die Umgebungsvariable *DISPLAY* festgelegt ist, sollten Sie *unset DISPLAY* ausführen und dann versuchen, das Plug-In manuell zu installieren.

## Schritte

1. Laden Sie das SnapCenter Plug-ins-Paket für AIX vom Installationsort des SnapCenter Servers herunter.

Der Standardinstallationspfad ist *C:\ProgramData\NetApp\ SnapCenter\PackageRepository*. Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.
3. Laufen

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
```

```

DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path-
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user

```

4. Bearbeiten Sie die Datei `spl.properties` unter `/var/opt/snapcenter/spl/etc/`, um `SPL_ENABLED_PLUGINS=SCO,SCU` hinzuzufügen, und starten Sie dann den Dienst SnapCenter Plug-in Loader neu.



Durch die Installation des Plug-In-Pakets werden die Plug-Ins auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie sollten die Plug-Ins auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter -GUI oder des PowerShell-Cmdlets hinzufügen. Wählen Sie beim Hinzufügen des Hosts „Keine“ als Anmeldeinformationen aus. Nachdem der Host hinzugefügt wurde, werden die installierten Plug-Ins automatisch erkannt.

## Konfigurieren des SnapCenter Plug-in Loader -Dienstes

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

### Über diese Aufgabe

Nach der Installation des SnapCenter Plug-ins-Pakets für Linux oder des SnapCenter Plug-ins-Pakets für AIX 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     | <p>Zeigt die unterstützten Protokollebenen an.</p> <p>Die möglichen Werte sind TRACE, DEBUG, INFO, WARN, ERROR und FATAL.</p>                                                              |
| SPL_PROTOCOL  | <p>Zeigt das vom SnapCenter Plug-in Loader unterstützte Protokoll an.</p> <p>Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.</p> |

| Parametername               | Beschreibung                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNAPCENTER_SERVER_PROTOKOLL | <p>Zeigt das vom SnapCenter Server unterstützte Protokoll an.</p> <p>Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.</p>                                                                                                                                                                    |
| SKIP_JAVAHOME_UPDATE        | <p>Standardmäßig erkennt der SPL-Dienst den Java-Pfad und aktualisiert den JAVA_HOME-Parameter.</p> <p>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.</p>                                                                    |
| SPL_KEYSTORE_PASS           | <p>Zeigt das Passwort der Keystore-Datei an.</p> <p>Sie können diesen Wert nur ändern, wenn Sie das Kennwort ändern oder eine neue Keystore-Datei erstellen.</p>                                                                                                                                                                                      |
| SPL_PORT                    | <p>Zeigt die Portnummer an, auf der der SnapCenter Plug-in Loader -Dienst ausgeführt wird.</p> <p>Sie können den Wert hinzufügen, wenn der Standardwert fehlt.</p> <div>  <p>Sie sollten den Wert nach der Installation der Plug-Ins nicht mehr ändern.</p> </div> |
| SNAPCENTER_SERVER_HOST      | <p>Zeigt die IP-Adresse oder den Hostnamen des SnapCenter -Servers an.</p>                                                                                                                                                                                                                                                                            |
| SPL_KEYSTORE_PATH           | <p>Zeigt den absoluten Pfad der Keystore-Datei an.</p>                                                                                                                                                                                                                                                                                                |
| SNAPCENTER_SERVER_PORT      | <p>Zeigt die Portnummer an, auf der der SnapCenter -Server ausgeführt wird.</p>                                                                                                                                                                                                                                                                       |

| Parametername                           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOGS_MAX_COUNT                          | <p>Zeigt die Anzahl der Protokolldateien des SnapCenter Plug-in Loader an, die im Ordner <code>/custom_location/snapcenter/spl/logs</code> gespeichert sind.</p> <p>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.</p> <div>  <p>Wenn Sie die Datei „spl.properties“ manuell löschen, wird die Anzahl der beizubehaltenden Dateien auf 9999 festgelegt.</p> </div> |
| JAVA_HOME                               | <p>Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird.</p> <p>Dieser Pfad wird während der Installation und beim Starten von SPL festgelegt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG_MAX_SIZE                            | <p>Zeigt die maximale Größe der Job-Protokolldatei an.</p> <p>Sobald die maximale Größe erreicht ist, wird die Protokolldatei komprimiert und die Protokolle in die neue Datei dieses Auftrags geschrieben.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Protokolle der letzten Tage aufbewahren | <p>Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Zertifikatsvalidierung aktivieren       | <p>Zeigt „true“ an, wenn die CA-Zertifikatsvalidierung für den Host aktiviert ist.</p> <p>Sie können diesen Parameter entweder durch Bearbeiten der spl.properties oder mithilfe der SnapCenter -GUI oder des Cmdlets aktivieren oder deaktivieren.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |

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  
<AliasNameForCertificateToBeImported> -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 Schlüsselspeicherkenwort.

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 "<OriginalAliasName>" -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.

## Importieren Sie Daten aus SnapManager für Oracle und SnapManager für SAP in SnapCenter

Durch das Importieren von Daten aus SnapManager für Oracle und SnapManager für SAP in SnapCenter können Sie Ihre Daten aus früheren Versionen weiterhin verwenden.

Sie können Daten von SnapManager für Oracle und SnapManager für SAP in SnapCenter importieren, indem Sie das Importtool über die Befehlszeilenschnittstelle (Linux-Host-CLI) ausführen.

Das Importtool erstellt Richtlinien und Ressourcengruppen in SnapCenter. Die in SnapCenter erstellten Richtlinien und Ressourcengruppen entsprechen den Profilen und Vorgängen, die mit diesen Profilen in SnapManager für Oracle und SnapManager für SAP ausgeführt werden. Das SnapCenter Importtool interagiert mit den Repository-Datenbanken SnapManager für Oracle und SnapManager für SAP und der Datenbank, die Sie importieren möchten.

- Ruft alle Profile, Zeitpläne und Vorgänge ab, die mit den Profilen ausgeführt wurden.
- Erstellt eine SnapCenter -Sicherungsrichtlinie für jeden einzelnen Vorgang und jeden Zeitplan, der einem Profil zugeordnet ist.
- Erstellt eine Ressourcengruppe für jede Zieldatenbank.

Sie können das Importtool ausführen, indem Sie das Skript `sc-migrate` unter `/opt/NetApp/snapcenter/spl/bin` ausführen. Wenn Sie das SnapCenter Plug-ins-Paket für Linux auf dem Datenbankhost installieren, den Sie importieren möchten, wird das Skript `sc-migrate` nach `/opt/NetApp/snapcenter/spl/bin` kopiert.



Das Importieren von Daten wird von der grafischen Benutzeroberfläche (GUI) von SnapCenter nicht unterstützt.

SnapCenter unterstützt Data ONTAP im 7-Modus nicht. Mit dem 7-Mode Transition Tool können Sie Daten und Konfigurationen, die auf einem System mit Data ONTAP im 7-Mode gespeichert sind, auf ein ONTAP -System migrieren.

### Unterstützte Konfigurationen für den Datenimport

Bevor Sie Daten von SnapManager 3.4.x für Oracle und SnapManager 3.4.x für SAP in SnapCenter importieren, sollten Sie sich über die Konfigurationen im Klaren sein, die mit dem SnapCenter -Plug-in für Oracle-Datenbanken unterstützt werden.

Die Konfigurationen, die mit dem SnapCenter Plug-in für Oracle Database unterstützt werden, sind in der ["NetApp Interoperabilitätsmatrix-Tool"](#) .

### Was wird in SnapCenter importiert?

Sie können Profile, Zeitpläne und mithilfe der Profile durchgeführte Vorgänge importieren.

| Von SnapManager für Oracle und SnapManager für SAP       | Zu SnapCenter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile ohne Operationen und Zeitpläne                   | Es wird eine Richtlinie mit dem Standardsicherungstyp „Online“ und dem Sicherungsumfang „Vollständig“ erstellt.                                                                                                                                                                                                                                                                                                                                                                                             |
| Profile mit einer oder mehreren Operationen              | <p>Mehrere Richtlinien werden basierend auf einer einzigartigen Kombination aus einem Profil und den mit diesem Profil ausgeführten Vorgängen erstellt.</p> <p>Die in SnapCenter erstellten Richtlinien enthalten die aus dem Profil und den entsprechenden Vorgängen abgerufenen Details zum Bereinigen und Aufbewahren des Archivprotokolls.</p>                                                                                                                                                          |
| Profile mit Oracle Recovery Manager (RMAN)-Konfiguration | <p>Richtlinien werden mit aktivierter Option <b>Katalogsicherung mit Oracle Recovery Manager</b> erstellt.</p> <p>Wenn in SnapManager eine externe RMAN-Katalogisierung verwendet wurde, müssen Sie die RMAN-Katalogeinstellungen in SnapCenter konfigurieren. Sie können entweder die vorhandenen Anmeldeinformationen auswählen oder neue Anmeldeinformationen erstellen.</p> <p>Wenn RMAN über die Steuerdatei in SnapManager konfiguriert wurde, müssen Sie RMAN nicht in SnapCenter konfigurieren.</p> |
| An ein Profil angehängter Zeitplan                       | Es wird eine Richtlinie nur für den Zeitplan erstellt.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Datenbank                                                | <p>Für jede importierte Datenbank wird eine Ressourcengruppe erstellt.</p> <p>In einem Real Application Clusters (RAC)-Setup wird der Knoten, auf dem Sie das Importtool ausführen, nach dem Import zum bevorzugten Knoten und die Ressourcengruppe wird für diesen Knoten erstellt.</p>                                                                                                                                                                                                                    |



Beim Importieren eines Profils wird zusammen mit der Sicherungsrichtlinie eine Überprüfungsrichtlinie erstellt.

Wenn SnapManager für Oracle und SnapManager für SAP-Profiles, Zeitpläne und alle mit den Profilen ausgeführten Vorgänge in SnapCenter importiert werden, werden auch die verschiedenen Parameterwerte importiert.

| <b>SnapManager für Oracle und SnapManager für SAP-Parameter und -Werte</b>                                                                                                                                                                          | <b>SnapCenter -Parameter und -Werte</b>                                                                                                                                    | <b>Hinweise</b>                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Sicherungsumfang</p> <ul style="list-style-type: none"> <li>• Voll</li> <li>• Daten</li> <li>• Protokoll</li> </ul>                                                                                                                              | <p>Sicherungsumfang</p> <ul style="list-style-type: none"> <li>• Voll</li> <li>• Daten</li> <li>• Protokoll</li> </ul>                                                     |                                                                                                                                                                                                                                                                                                                                                  |
| <p>Backup-Modus</p> <ul style="list-style-type: none"> <li>• Automatisch</li> <li>• Online</li> <li>• Offline</li> </ul>                                                                                                                            | <p>Sicherungstyp</p> <ul style="list-style-type: none"> <li>• Online</li> <li>• Offline-Herunterfahren</li> </ul>                                                          | <p>Wenn der Sicherungsmodus „Auto“ ist, überprüft das Importtool den Datenbankstatus zum Zeitpunkt der Ausführung des Vorgangs und legt den Sicherungstyp entsprechend auf „Online-Herunterfahren“ oder „Offline-Herunterfahren“ fest.</p>                                                                                                       |
| <p>Zurückbehaltung</p> <ul style="list-style-type: none"> <li>• Tage</li> <li>• Zählt</li> </ul>                                                                                                                                                    | <p>Zurückbehaltung</p> <ul style="list-style-type: none"> <li>• Tage</li> <li>• Zählt</li> </ul>                                                                           | <p>SnapManager für Oracle und SnapManager für SAP verwenden sowohl Tage als auch Zählwerte, um die Aufbewahrung festzulegen.</p> <p>In SnapCenter gibt es entweder Tage <i>ODER</i> Zählungen. Daher wird die Aufbewahrung in Tagen festgelegt, da die Tage Vorrang vor der Zählung in SnapManager für Oracle und SnapManager für SAP haben.</p> |
| <p>Beschneiden für Zeitpläne</p> <ul style="list-style-type: none"> <li>• Alle</li> <li>• Systemänderungsnummer (SCN)</li> <li>• Datum</li> <li>• Protokolle, die vor den angegebenen Stunden, Tagen, Wochen und Monaten erstellt wurden</li> </ul> | <p>Beschneiden für Zeitpläne</p> <ul style="list-style-type: none"> <li>• Alle</li> <li>• Protokolle, die vor den angegebenen Stunden und Tagen erstellt wurden</li> </ul> | <p>SnapCenter unterstützt kein Beschneiden basierend auf SCN, Datum, Wochen und Monaten.</p>                                                                                                                                                                                                                                                     |

| <b>SnapManager für Oracle und SnapManager für SAP-Parameter und -Werte</b>                                                                                                                                                                                                                                    | <b>SnapCenter -Parameter und -Werte</b>                                                                                                            | <b>Hinweise</b>                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Benachrichtigung</p> <ul style="list-style-type: none"> <li>• E-Mails werden nur bei erfolgreichen Vorgängen gesendet</li> <li>• E-Mails werden nur bei fehlgeschlagenen Vorgängen gesendet</li> <li>• E-Mails werden sowohl bei erfolgreichen als auch bei fehlgeschlagenen Vorgängen gesendet</li> </ul> | <p>Benachrichtigung</p> <ul style="list-style-type: none"> <li>• Stets</li> <li>• Bei einem Fehler</li> <li>• Warnung</li> <li>• Fehler</li> </ul> | <p>Die E-Mail-Benachrichtigungen werden importiert.</p> <p>Sie müssen den SMTP-Server jedoch manuell über die SnapCenter -GUI aktualisieren. Der Betreff der E-Mail bleibt leer, damit Sie ihn konfigurieren können.</p> |

### **Was nicht in SnapCenter importiert wird**

Das Importtool importiert nicht alles in SnapCenter.

Folgendes können Sie nicht in SnapCenter importieren:

- Metadaten sichern
- Teilsicherungen
- Raw Device Mapping (RDM) und Virtual Storage Console (VSC) bezogene Backups
- Rollen oder alle im SnapManager für Oracle und SnapManager für SAP-Repository verfügbaren Anmeldeinformationen
- Daten im Zusammenhang mit Überprüfungs-, Wiederherstellungs- und Klonvorgängen
- Beschneiden für den Betrieb
- Im SnapManager für Oracle- und SnapManager für SAP-Profil angegebene Replikationsdetails

Nach dem Importieren müssen Sie die entsprechende in SnapCenter erstellte Richtlinie manuell bearbeiten, um die Replikationsdetails einzuschließen.

- Katalogisierte Sicherungsinformationen

### **Vorbereiten des Datenimports**

Bevor Sie Daten in SnapCenter importieren, müssen Sie bestimmte Aufgaben ausführen, um den Importvorgang erfolgreich auszuführen.

#### **Schritte**

1. Identifizieren Sie die Datenbank, die Sie importieren möchten.
2. Fügen Sie mithilfe von SnapCenter den Datenbankhost hinzu und installieren Sie das SnapCenter Plug-ins-Paket für Linux.
3. Richten Sie mithilfe von SnapCenter die Verbindungen für die von den Datenbanken auf dem Host verwendeten Storage Virtual Machines (SVMs) ein.

4. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
5. Stellen Sie auf der Seite „Ressourcen“ sicher, dass die zu importierende Datenbank erkannt und angezeigt wird.

Wenn Sie das Importtool ausführen möchten, muss auf die Datenbank zugegriffen werden können, sonst schlägt die Erstellung der Ressourcengruppe fehl.

Wenn für die Datenbank Anmeldeinformationen konfiguriert sind, müssen Sie in SnapCenter entsprechende Anmeldeinformationen erstellen, die Anmeldeinformationen der Datenbank zuweisen und dann die Erkennung der Datenbank erneut ausführen. Wenn sich die Datenbank auf Automatic Storage Management (ASM) befindet, müssen Sie Anmeldeinformationen für die ASM-Instanz erstellen und die Anmeldeinformationen der Datenbank zuweisen.

6. Stellen Sie sicher, dass der Benutzer, der das Importtool ausführt, über ausreichende Berechtigungen verfügt, um SnapManager für Oracle- oder SnapManager für SAP-CLI-Befehle (wie den Befehl zum Anhalten von Zeitplänen) vom SnapManager für Oracle- oder SnapManager für SAP-Host aus auszuführen.
7. Führen Sie die folgenden Befehle auf dem SnapManager für Oracle- oder SnapManager für SAP-Host aus, um die Zeitpläne auszusetzen:
  - a. Wenn Sie die Zeitpläne auf dem SnapManager für Oracle-Host aussetzen möchten, führen Sie Folgendes aus:

- `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smo credential set -profile -name profile_name`



Sie müssen den Befehl „smo credential set“ für jedes Profil auf dem Host ausführen.

- b. Wenn Sie die Zeitpläne auf dem SnapManager für SAP-Host aussetzen möchten, führen Sie Folgendes aus:

- `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smsap credential set -profile -name profile_name`



Sie müssen den Befehl „Smsap Credential Set“ für jedes Profil auf dem Host ausführen.

8. Stellen Sie sicher, dass der vollqualifizierte Domänenname (FQDN) des Datenbankhosts angezeigt wird, wenn Sie `hostname -f` ausführen.

Wenn der FQDN nicht angezeigt wird, müssen Sie `/etc/hosts` ändern, um den FQDN des Hosts anzugeben.

## Daten importieren

Sie können Daten importieren, indem Sie das Importtool vom Datenbankhost ausführen.

## Über diese Aufgabe

Die nach dem Import erstellten SnapCenter -Sicherungsrichtlinien haben unterschiedliche Namensformate:

- Für Profile ohne Vorgänge und Zeitpläne erstellte Richtlinien haben das Format `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED`.

Wenn kein Vorgang mithilfe eines Profils ausgeführt wird, wird die entsprechende Richtlinie mit dem Standardsicherungstyp „Online“ und dem Sicherungsumfang „Vollständig“ erstellt.

- Für die Profile mit einem oder mehreren Vorgängen erstellte Richtlinien haben das Format `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.
- Für die an die Profile angehängten Zeitpläne erstellte Richtlinien haben das Format `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`.

## Schritte

1. Melden Sie sich beim Datenbankhost an, den Sie importieren möchten.
2. Führen Sie das Importtool aus, indem Sie das Skript `sc-migrate` unter `/opt/NetApp/snapcenter/spl/bin` ausführen.
3. Geben Sie den Benutzernamen und das Kennwort des SnapCenter -Servers ein.

Nach der Validierung der Anmeldeinformationen wird eine Verbindung mit SnapCenter hergestellt.

4. Geben Sie die Repository-Datenbankdetails von SnapManager für Oracle oder SnapManager für SAP ein.

Die Repository-Datenbank listet die Datenbanken auf, die auf dem Host verfügbar sind.

5. Geben Sie die Details der Zieldatenbank ein.

Wenn Sie alle Datenbanken auf dem Host importieren möchten, geben Sie „all“ ein.

6. Wenn Sie ein Systemprotokoll erstellen oder ASUP-Nachrichten für fehlgeschlagene Vorgänge senden möchten, müssen Sie diese entweder durch Ausführen des Befehls `Add-SmStorageConnection` oder `Set-SmStorageConnection` aktivieren.



Wenn Sie einen Importvorgang abbrechen möchten, entweder während der Ausführung des Importtools oder nach dem Importieren, müssen Sie die SnapCenter -Richtlinien, Anmeldeinformationen und Ressourcengruppen, die im Rahmen des Importvorgangs erstellt wurden, manuell löschen.

## Ergebnisse

Die SnapCenter -Sicherungsrichtlinien werden für Profile, Zeitpläne und Vorgänge erstellt, die mithilfe der Profile ausgeführt werden. Für jede Zieldatenbank werden außerdem Ressourcengruppen erstellt.



Nach dem erfolgreichen Importieren der Daten werden die mit der importierten Datenbank verknüpften Zeitpläne in SnapManager für Oracle und SnapManager für SAP angehalten.



Nach dem Importieren müssen Sie die importierte Datenbank oder das Dateisystem mit SnapCenter verwalten.

Die Protokolle für jede Ausführung des Importtools werden im Verzeichnis `/var/opt/snapcenter/spl/logs` unter dem Namen `spl_migration_timestamp.log` gespeichert. Sie können dieses Protokoll verwenden, um Importfehler zu überprüfen und zu beheben.

## 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.

## Vorbereiten des Schutzes von Oracle-Datenbanken

Bevor Sie Datenschutzvorgänge wie Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen, müssen Sie Ihre Strategie definieren und die 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 Oracle Database 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.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus „Linux“ oder „AIX“ für den Installationsbenutzer. "[Mehr erfahren](#)"
- Fügen Sie Hosts hinzu, installieren Sie die Plug-Ins und entdecken Sie die Ressourcen.
- Wenn Sie SnapCenter Server zum Schutz von Oracle-Datenbanken 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- oder AIX-Host.

Sehen "[Linux-Hostanforderungen](#)" oder "[AIX-Hostanforderungen](#)" für weitere Informationen.

- Sie sollten den Timeout-Wert der Anwendungsfirewall auf 3 Stunden oder mehr einstellen.
- Wenn Sie Oracle-Datenbanken in NFS-Umgebungen haben, müssen Sie mindestens ein NFS-Daten-LIF für den primären oder sekundären Speicher konfiguriert haben, um Mount-, Klon-, Überprüfungs- und Wiederherstellungsvorgänge durchzuführen.
- Wenn Sie über mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration verfügen, können Sie mithilfe der SnapCenter -CLI auf dem Datenbankhost Folgendes ausführen:
  - Standardmäßig werden alle IP-Adressen des Datenbankhosts zur NFS-Speicherexportrichtlinie in der Storage Virtual Machine (SVM) für die geklonten Volumes hinzugefügt. Wenn Sie eine bestimmte IP-Adresse haben oder auf eine Teilmenge der IP-Adressen beschränken möchten, führen Sie die CLI „Set-PreferredHostIPsInStorageExportPolicy“ aus.
  - Wenn Sie in SVM über mehrere Datenpfade (LIFs) verfügen, wählt SnapCenter den entsprechenden Datenpfad (LIF) zum Mounten des geklonten NFS-Volumes aus. Wenn Sie jedoch einen bestimmten Datenpfad (LIF) angeben möchten, müssen Sie die CLI „Set-SvmPreferredDataPath“ ausführen. Weitere Informationen finden Sie im Befehlsreferenzhandbuch.
- Wenn Sie Oracle-Datenbanken in SAN-Umgebungen haben, stellen Sie sicher, dass die SAN-Umgebung gemäß den Empfehlungen in den folgenden Anleitungen konfiguriert ist:
  - "[Verwenden von Linux-Hosts mit ONTAP -Speicher](#)"
  - "[Von AIX-Host-Dienstprogrammen betroffene Hosteinstellungen](#)"
- Wenn Sie Oracle-Datenbanken auf LVM in den Betriebssystemen Oracle Linux oder RHEL haben, installieren Sie die neueste Version von Logical Volume Management (LVM).
- Wenn Sie SnapManager für Oracle verwenden und zum SnapCenter Plug-in für Oracle Database migrieren möchten, können Sie die Profile mit dem sccli-Befehl sc-migrate in Richtlinien und Ressourcengruppen von SnapCenter migrieren.
- Konfigurieren Sie SnapMirror und SnapVault auf ONTAP, wenn Sie eine Backup-Replikation wünschen

Für Benutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.1.1 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme. Für Benutzer von SnapCenter 4.2.x sowie NetApp Data Broker 1.0 und 1.0.1 enthält die Dokumentation Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des SnapCenter Plug-in for VMware vSphere, das von der Linux-basierten virtuellen NetApp Data Broker-Appliance (Open Virtual Appliance-Format) bereitgestellt wird. Für Benutzer von SnapCenter 4.3.x enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des Linux-basierten SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance-Format).

## Weitere Informationen finden

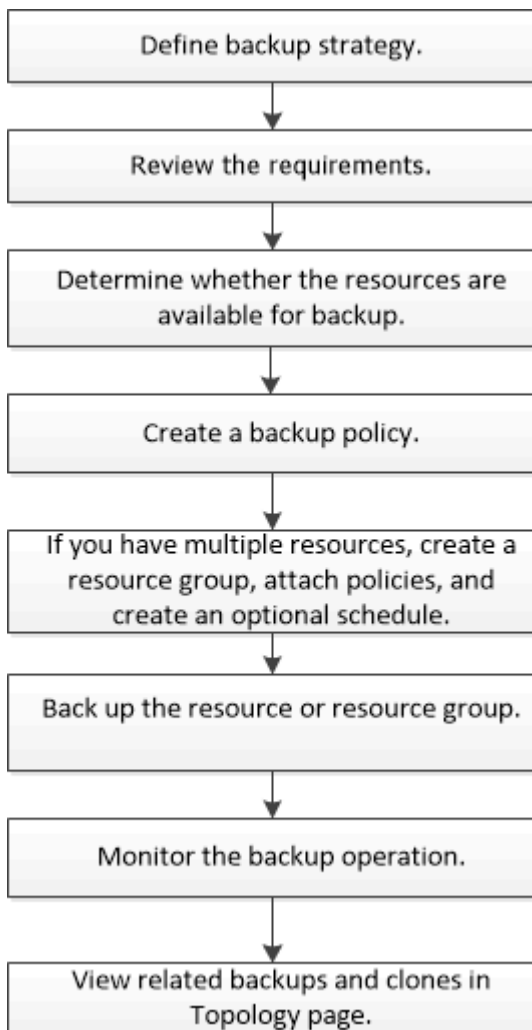
- ["Interoperabilitätsmatrix-Tool"](#)
- ["SnapCenter Plug-in for VMware vSphere Dokumentation"](#)
- ["Der Datenschutzvorgang schlägt in einer Umgebung ohne Multipath in RHEL 7 und höher fehl"](#)

# Sichern Sie Oracle-Datenbanken

## Übersicht über das Backup-Verfahren

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Das Sicherungsverfahren umfasst die Planung, die Identifizierung der Ressourcen für die Sicherung, die Erstellung von Sicherungsrichtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Beim Erstellen einer Sicherung für Oracle-Datenbanken wird auf dem Oracle-Datenbankhost im Verzeichnis `/var/opt/snapcenter/sco/lock` eine Betriebssperredatei (`.sm_lock_dbsid`) erstellt, um zu vermeiden, dass mehrere Vorgänge auf der Datenbank ausgeführt werden. Nach der Sicherung der Datenbank wird die

Betriebssperrdatei automatisch entfernt.

Wenn die vorherige Sicherung jedoch mit einer Warnung abgeschlossen wurde, wird die Betriebssperrdatei möglicherweise nicht gelöscht und der nächste Sicherungsvorgang wird in die Warteschlange gestellt. Es kann eventuell abgebrochen werden, wenn die Datei **.sm\_lock\_dbsid** nicht gelöscht wird. In einem solchen Szenario müssen Sie die Betriebssperrdatei manuell löschen, indem Sie die folgenden Schritte ausführen:

1. Navigieren Sie in der Eingabeaufforderung zu `/var/opt/snapcenter/sco/lock`.
2. Löschen der Betriebssperre: `rm -rf .sm_lock_dbsid`.

## Informationen zur Sicherungskonfiguration

### Unterstützte Oracle-Datenbankkonfigurationen für Backups

SnapCenter unterstützt die Sicherung verschiedener Oracle-Datenbankkonfigurationen.

- Oracle Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container Database (CDB)
- Oracle Data Guard-Standby

Sie können nur Offline-Mount-Backups von Data Guard-Standbydatenbanken erstellen. Offline-Shutdown-Backup, reine Archivprotokoll-Backup und vollständige Backups werden nicht unterstützt.

- Oracle Active Data Guard-Standby

Sie können nur Online-Backups von Active Data Guard-Standbydatenbanken erstellen. Nur Archivprotokollsicherungen und vollständige Sicherungen werden nicht unterstützt.

Vor dem Erstellen einer Sicherung der Data Guard-Standby- oder Active Data Guard-Standby-Datenbank wird der verwaltete Wiederherstellungsprozess (MRP) gestoppt und nach der Erstellung der Sicherung wird MRP gestartet.

- Automatisches Speichermanagement (ASM)
  - ASM Standalone und ASM RAC auf Virtual Machine Disk (VMDK)

Unter allen für Oracle-Datenbanken unterstützten Wiederherstellungsmethoden können Sie auf VMDK nur eine Connect-and-Copy-Wiederherstellung von ASM RAC-Datenbanken durchführen.

- ASM Standalone und ASM RAC auf Raw Device Mapping (RDM) + Sie können Sicherungs-, Wiederherstellungs- und Klonvorgänge für Oracle-Datenbanken auf ASM durchführen, mit oder ohne ASMLib.
- Oracle ASM-Filtertreiber (ASMFD)

PDB-Migrations- und PDB-Klonvorgänge werden nicht unterstützt.

- Oracle Flex ASM

Die neuesten Informationen zu unterstützten Oracle-Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#).

## Unterstützte Sicherungstypen für Oracle-Datenbanken

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt Online- und Offline-Sicherungstypen für Oracle-Datenbanken.

### Online-Backup

Eine Sicherung, die erstellt wird, wenn sich die Datenbank im Online-Zustand befindet, wird als Online-Sicherung bezeichnet. Mit einem Online-Backup, auch Hot-Backup genannt, können Sie eine Sicherung der Datenbank erstellen, ohne diese herunterzufahren.

Im Rahmen der Online-Sicherung können Sie eine Sicherung der folgenden Dateien erstellen:

- Nur Datendateien und Steuerdateien
- Nur Protokolldateien archivieren (die Datenbank wird in diesem Szenario nicht in den Sicherungsmodus versetzt)
- Vollständige Datenbank, die Datendateien, Steuerdateien und Archivprotokolldateien enthält

### Offline-Backup

Eine Sicherung, die erstellt wird, während sich die Datenbank entweder im gemounteten oder heruntergefahrenen Zustand befindet, wird als Offline-Sicherung bezeichnet. Ein Offline-Backup wird auch als Cold Backup bezeichnet. Sie können in Offline-Backups nur Datendateien und Steuerdateien einschließen. Sie können entweder eine Offline-Mount- oder eine Offline-Shutdown-Sicherung erstellen.

- Beim Erstellen einer Offline-Mount-Sicherung müssen Sie sicherstellen, dass sich die Datenbank in einem gemounteten Zustand befindet.

Wenn sich die Datenbank in einem anderen Zustand befindet, schlägt der Sicherungsvorgang fehl.

- Beim Erstellen einer Offline-Shutdown-Sicherung kann sich die Datenbank in einem beliebigen Zustand befinden.

Der Datenbankstatus wird in den erforderlichen Status geändert, um eine Sicherung zu erstellen. Nach dem Erstellen des Backups wird der Datenbankzustand in den ursprünglichen Zustand zurückgesetzt.

## So erkennt SnapCenter Oracle-Datenbanken

Ressourcen sind Oracle-Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Sie können diese Datenbanken zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

In den folgenden Abschnitten wird der Prozess beschrieben, den SnapCenter zum Erkennen verschiedener Typen und Versionen von Oracle-Datenbanken verwendet.

### Für Oracle-Versionen 11g bis 12cR1

#### RAC-Datenbank

Die RAC-Datenbanken werden nur auf der Grundlage von `/etc/oratab`-Einträgen erkannt. Sie sollten die Datenbankeinträge in der Datei `/etc/oratab` haben.

## **Eigenständig**

Die eigenständigen Datenbanken werden nur auf der Grundlage von /etc/oratab-Einträgen erkannt.

## **ASM**

Der ASM-Instanzeintrag sollte in der Datei /etc/oratab verfügbar sein.

## **RAC Ein Knoten**

Die RAC One Node-Datenbanken werden nur auf der Grundlage von /etc/oratab-Einträgen erkannt. Die Datenbanken sollten sich entweder im Status „nomount“, „mount“ oder „open“ befinden. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Der Datenbankstatus von RAC One Node wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt wurde und Sicherungen mit der Datenbank verknüpft sind.

Bei einer Datenbankverlagerung sollten Sie folgende Schritte durchführen:

1. Fügen Sie den verschobenen Datenbankeintrag manuell in die Datei /etc/oratab auf dem fehlgeschlagenen RAC-Knoten ein.
2. Aktualisieren Sie die Ressourcen manuell.
3. Wählen Sie auf der Ressourcenseite die RAC One Node-Datenbank aus und klicken Sie dann auf Datenbankeinstellungen.
4. Konfigurieren Sie die Datenbank, um die bevorzugten Clusterknoten auf den RAC-Knoten festzulegen, der derzeit die Datenbank hostet.
5. Führen Sie die SnapCenter -Vorgänge durch.
6. Wenn Sie eine Datenbank von einem Knoten auf einen anderen Knoten verschoben haben und der oratab-Eintrag im vorherigen Knoten nicht gelöscht wurde, löschen Sie den oratab-Eintrag manuell, um zu vermeiden, dass dieselbe Datenbank zweimal angezeigt wird.

## **Für Oracle-Versionen 12cR2 bis 18c, 19c oder 21c**

## **RAC-Datenbank**

Die RAC-Datenbanken werden mit dem Befehl „srvctl config“ erkannt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

## **Eigenständig**

Die eigenständigen Datenbanken werden anhand der Einträge in der Datei /etc/oratab und der Ausgabe des Befehls „srvctl config“ erkannt.

## **ASM**

Der ASM-Instanzeintrag muss nicht in der Datei /etc/oratab enthalten sein.

## **RAC Ein Knoten**

Die RAC One Node-Datenbanken werden nur mit dem Befehl „srvctl config“ erkannt. Die Datenbanken sollten sich entweder im Status „nomount“, „mount“ oder „open“ befinden. Der Datenbankstatus von RAC One Node wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt wurde und Sicherungen mit der Datenbank verknüpft sind.

Bei einer Verlagerung der Datenbank sollten Sie folgende Schritte durchführen: . Aktualisieren Sie die Ressourcen manuell. . Wählen Sie auf der Ressourcenseite die RAC One Node-Datenbank aus und klicken Sie dann auf Datenbankeinstellungen. . Konfigurieren Sie die Datenbank, um die bevorzugten Clusterknoten auf den RAC-Knoten festzulegen, der derzeit die Datenbank hostet. . Führen Sie die SnapCenter -Vorgänge

durch.



Wenn in der Datei `/etc/oratab` Oracle 12cR2- und 18c-Datenbankeinträge vorhanden sind und dieselbe Datenbank mit dem Befehl `srvctl config` registriert ist, entfernt SnapCenter die doppelten Datenbankeinträge. Wenn veraltete Datenbankeinträge vorhanden sind, wird die Datenbank zwar erkannt, ist jedoch nicht erreichbar und hat den Status „Offline“.

## Bevorzugte Knoten im RAC-Setup

Beim Einrichten von Oracle Real Application Clusters (RAC) können Sie die bevorzugten Knoten angeben, die SnapCenter zum Ausführen des Sicherungsvorgangs verwendet. Wenn Sie den bevorzugten Knoten nicht angeben, weist SnapCenter automatisch einen Knoten als bevorzugten Knoten zu und die Sicherung wird auf diesem Knoten erstellt.

Bei den bevorzugten Knoten kann es sich um einen oder alle Clusterknoten handeln, auf denen die RAC-Datenbankinstanzen vorhanden sind. Der Sicherungsvorgang wird nur auf diesen bevorzugten Knoten in der Reihenfolge der Präferenz ausgelöst.

### Beispiel

Die RAC-Datenbank `cdbrac` hat drei Instanzen: `cdbrac1` auf Knoten1, `cdbrac2` auf Knoten2 und `cdbrac3` auf Knoten3.

Die Instanzen `node1` und `node2` werden als bevorzugte Knoten konfiguriert, wobei `node2` die erste Präferenz und `node1` die zweite Präferenz ist. Wenn Sie einen Sicherungsvorgang durchführen, wird der Vorgang zuerst auf Knoten2 versucht, da dies der erste bevorzugte Knoten ist.

Wenn sich Knoten2 nicht im erforderlichen Status für die Sicherung befindet (was mehrere Gründe haben kann), z. B. dass der Plug-in-Agent auf dem Host nicht ausgeführt wird, die Datenbankinstanz auf dem Host sich nicht im erforderlichen Status für den angegebenen Sicherungstyp befindet oder die Datenbankinstanz auf Knoten2 in einer FlexASM-Konfiguration nicht von der lokalen ASM-Instanz bedient wird), wird der Vorgang auf Knoten1 versucht.

Der Knoten3 wird nicht für die Sicherung verwendet, da er nicht auf der Liste der bevorzugten Knoten steht.

## Flex ASM-Setup

In einem Flex ASM-Setup werden Leaf-Knoten nicht als bevorzugte Knoten aufgeführt, wenn die Kardinalität geringer ist als die Anzahl der Knoten im RAC-Cluster. Wenn sich die Knotenrollen des Flex ASM-Clusters ändern, sollten Sie dies manuell feststellen, damit die bevorzugten Knoten aktualisiert werden.

## Erforderlicher Datenbankstatus

Die RAC-Datenbankinstanzen auf den bevorzugten Knoten müssen sich im erforderlichen Zustand befinden, damit die Sicherung erfolgreich abgeschlossen werden kann:

- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im offenen Zustand befinden, um eine Onlinesicherung zu erstellen.
- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im Mount-Status befinden und alle anderen Instanzen, einschließlich anderer bevorzugter Knoten, müssen sich im Mount-Status oder niedriger befinden, um eine Offline-Mount-Sicherung zu erstellen.
- RAC-Datenbankinstanzen können sich in jedem beliebigen Zustand befinden, Sie müssen jedoch die bevorzugten Knoten angeben, um eine Offline-Shutdown-Sicherung zu erstellen.

## So katalogisieren Sie Backups mit Oracle Recovery Manager

Sie können die Sicherungen von Oracle-Datenbanken mit Oracle Recovery Manager (RMAN) katalogisieren, um die Sicherungsinformationen im Oracle RMAN-Repository zu speichern.

Die katalogisierten Sicherungen können später für die Wiederherstellung auf Blockebene oder für Point-in-Time-Wiederherstellungsvorgänge im Tablespace verwendet werden. Wenn Sie diese katalogisierten Sicherungen nicht benötigen, können Sie die Kataloginformationen entfernen.

Für die Katalogisierung muss die Datenbank im gemounteten oder höheren Zustand sein. Sie können Datensicherungen, Archivprotokollsicherungen und vollständige Sicherungen katalogisieren. Wenn die Katalogisierung für die Sicherung einer Ressourcengruppe mit mehreren Datenbanken aktiviert ist, wird die Katalogisierung für jede Datenbank durchgeführt. Bei Oracle RAC-Datenbanken wird die Katalogisierung auf dem bevorzugten Knoten durchgeführt, auf dem sich die Datenbank zumindest im gemounteten Zustand befindet.

Wenn Sie Sicherungen einer RAC-Datenbank katalogisieren möchten, stellen Sie sicher, dass für diese Datenbank kein anderer Job ausgeführt wird. Wenn ein anderer Job ausgeführt wird, schlägt der Katalogisierungsvorgang fehl, anstatt in die Warteschlange gestellt zu werden.

### Externe Katalogdatenbank

Standardmäßig wird die Steuerdatei der Zieldatenbank für die Katalogisierung verwendet. Wenn Sie eine externe Katalogdatenbank hinzufügen möchten, können Sie diese konfigurieren, indem Sie die Anmeldeinformationen und den Transparent Network Substrate (TNS)-Namen des externen Katalogs mithilfe des Datenbankeinstellungsassistenten der grafischen Benutzeroberfläche (GUI) von SnapCenter angeben. Sie können die externe Katalogdatenbank auch über die CLI konfigurieren, indem Sie den Befehl `Configure-SmOracleDatabase` mit den Optionen `-OracleRmanCatalogCredentialName` und `-OracleRmanCatalogTnsName` ausführen.

### RMAN-Befehl

Wenn Sie die Katalogisierungsoption beim Erstellen einer Oracle-Sicherungsrichtlinie über die SnapCenter -GUI aktiviert haben, werden die Sicherungen im Rahmen des Sicherungsvorgangs mit Oracle RMAN katalogisiert. Sie können auch eine verzögerte Katalogisierung von Backups durchführen, indem Sie den `Catalog-SmBackupWithOracleRMAN` Befehl.

Nach der Katalogisierung der Backups können Sie die `Get-SmBackupDetails` Befehl zum Abrufen der katalogisierten Sicherungsinformationen, z. B. des Tags für katalogisierte Datendateien, des Katalogpfads der Steuerdatei und der Speicherorte der katalogisierten Archivprotokolle.

### Benennungsformat

Wenn der Name der ASM-Datenträgergruppe größer oder gleich 16 Zeichen ist, lautet das für die Sicherung verwendete Namensformat ab SnapCenter 3.0 `SC_HASHCODEofDISKGROUP_DBSID_BACKUPID`. Wenn der Name der Datenträgergruppe jedoch weniger als 16 Zeichen umfasst, lautet das für die Sicherung verwendete Namensformat `DISKGROUPNAME_DBSID_BACKUPID`. Dies ist dasselbe Format, das in SnapCenter 2.0 verwendet wird.

Der `HASHCODEofDISKGROUP` ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Datenträgergruppe eindeutig ist.



## Crosscheck-Operationen

Sie können Gegenprüfungen durchführen, um veraltete RMAN-Repository-Informationen zu Sicherungen zu aktualisieren, deren Repository-Datensätze nicht mit ihrem physischen Status übereinstimmen. Wenn ein Benutzer beispielsweise archivierte Protokolle mit einem Betriebssystembefehl von der Festplatte entfernt, zeigt die Steuerdatei immer noch an, dass sich die Protokolle auf der Festplatte befinden, obwohl dies in Wirklichkeit nicht der Fall ist.

Durch die Gegenprüfung können Sie die Steuerdatei mit den Informationen aktualisieren. Sie können die Gegenprüfung aktivieren, indem Sie den Befehl „Set-SmConfigSettings“ ausführen und dem Parameter „ENABLE\_CROSSCHECK“ den Wert „TRUE“ zuweisen. Der Standardwert ist auf FALSE gesetzt.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

## Kataloginformationen entfernen

Sie können die Kataloginformationen entfernen, indem Sie den Befehl Uncatalog-SmBackupWithOracleRMAN ausführen. Sie können die Kataloginformationen nicht über die SnapCenter -GUI entfernen. Allerdings werden Informationen zu einer katalogisierten Sicherung entfernt, wenn die Sicherung gelöscht wird oder wenn die mit dieser katalogisierten Sicherung verknüpfte Aufbewahrungs- und Ressourcengruppe gelöscht wird.



Wenn Sie das Löschen des SnapCenter -Hosts erzwingen, werden die Informationen der mit diesem Host verknüpften katalogisierten Sicherungen nicht entfernt. Sie müssen Informationen aller katalogisierten Sicherungen für diesen Host entfernen, bevor Sie die Löschung des Hosts erzwingen.

Wenn das Katalogisieren und Entkatalogisieren fehlschlägt, weil die Vorgangszeit den für den Parameter ORACLE\_PLUGIN\_RMAN\_CATALOG\_TIMEOUT angegebenen Timeout-Wert überschritten hat, sollten Sie den Wert des Parameters ändern, indem Sie den folgenden Befehl ausführen:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType  
Plugin -PluginCode SCO-ConfigSettings  
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Nachdem Sie den Wert des Parameters geändert haben, starten Sie den Dienst SnapCenter Plug-in Loader (SPL) neu, indem Sie den folgenden Befehl ausführen:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von Get-Help command\_name. Alternativ können Sie sich an die ["SnapCenter Software-Befehlsreferenzhandbuch"](#) .

## Vordefinierte Umgebungsvariablen für backupspezifisches Prescript und Postscript

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie beim Erstellen von Sicherungsrichtlinien das Prescript und Postscript ausführen. Diese Funktionalität wird für alle Oracle-Konfigurationen außer VMDK unterstützt.

SnapCenter definiert die Werte der Parameter vor, auf die in der Umgebung, in der die Shell-Skripte ausgeführt werden, direkt zugegriffen werden kann. Sie müssen die Werte dieser Parameter beim Ausführen der Skripte

nicht manuell angeben.

#### Unterstützte vordefinierte Umgebungsvariablen zum Erstellen von Sicherungsrichtlinien

- **SC\_JOB\_ID** gibt die Job-ID des Vorgangs an.

Beispiel: 256

- **SC\_ORACLE\_SID** gibt die Systemkennung der Datenbank an.

Wenn der Vorgang mehrere Datenbanken umfasst, enthält der Parameter durch Pipe-Zeichen getrennte Datenbanknamen.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: NFSB32|NFSB31

- **SC\_HOST** gibt den Hostnamen der Datenbank an.

Bei RAC ist der Hostname der Name des Hosts, auf dem die Sicherung durchgeführt wird.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: scsmohost2.gdl.englabe.netapp.com

- **SC\_OS\_USER** gibt den Betriebssystembesitzer der Datenbank an.

Die Daten werden als <db1>@<osuser1>|<db2>@<osuser2> formatiert.

Beispiel: NFSB31@oracle|NFSB32@oracle

- **SC\_OS\_GROUP** gibt die Betriebssystemgruppe der Datenbank an.

Die Daten werden als <db1>@<osgroup1>|<db2>@<osgroup2> formatiert.

Beispiel: NFSB31@install|NFSB32@oinstall

- **SC\_BACKUP\_TYPE** gibt den Sicherungstyp an (Online-Vollsicherung, Online-Daten, Online-Protokoll, Offline-Herunterfahren, Offline-Mount)

Beispiele:

- Für vollständige Sicherung: ONLINEFULL
- Nur Datensicherung: ONLINEDATA
- Für reine Protokollsicherung: ONLINELOG

- **SC\_BACKUP\_NAME** gibt den Namen der Sicherung an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1|AV@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267

- **SC\_BACKUP\_ID** gibt die Sicherungs-ID an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: DATA@203|LOG@205|AV@207

- **SC\_ORACLE\_HOME** gibt den Pfad des Oracle-Home-Verzeichnisses an.

Beispiel:

NFSB32@/ora01/app/oracle/product/18.1.0/db\_1|NFSB31@/ora01/app/oracle/product/18.1.0/db\_1

- **SC\_BACKUP\_RETENTION** gibt den in der Richtlinie definierten Aufbewahrungszeitraum an.

Beispiele:

- Für vollständige Sicherung: Stündlich|DATA@DAYS:3|LOG@COUNT:4
- Für reine Datensicherung auf Abruf: Ondemand|DATA@COUNT:2
- Für On-Demand-Protokollsicherung: Ondemand|LOG@COUNT:2

- **SC\_RESOURCE\_GROUP\_NAME** gibt den Namen der Ressourcengruppe an.

Beispiel: RG1

- **SC\_BACKUP\_POLICY\_NAME** gibt den Namen der Sicherungsrichtlinie an.

Beispiel: backup\_policy

- **SC\_AV\_NAME** gibt die Namen der Anwendungsvolumes an.

Beispiel: AV1|AV2

- **SC\_PRIMARY\_DATA\_VOLUME\_FULL\_PATH** gibt die Speicherzuordnung von SVM zum Volume für das Datendateiverzeichnis an. Dies ist der Name des übergeordneten Volumes für LUNs und Qtrees.

Die Daten werden als <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2> formatiert.

Beispiele:

- Für 2 Datenbanken in derselben Ressourcengruppe:  
NFSB32@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA|NFSB31@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_DATA
- Für eine einzelne Datenbank mit Datendateien, die über mehrere Volumes verteilt sind:  
buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_DATA,herculus:/vol/scspr2417819002\_NFS

- **SC\_PRIMARY\_ARCHIVELOGS\_VOLUME\_FULL\_PATH** gibt die Speicherzuordnung von SVM zum Volume für das Protokolldateiverzeichnis an. Dies ist der Name des übergeordneten Volumes für LUNs und Qtrees.

Beispiele:

- Für einzelne Datenbankinstanz: buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_REDO
- Für mehrere Datenbankinstanzen:  
NFSB31@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_REDO|NFSB32@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO

- **SC\_PRIMARY\_FULL\_SNAPSHOT\_NAME\_FOR\_TAG** gibt die Liste der Snapshots an, die den Namen des Speichersystems und den Namen des Datenträgers enthalten.

Beispiele:

- Für einzelne Datenbankinstanz:  
buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1
  - Für mehrere Datenbankinstanzen:  
NFSB32@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1  
|NFSB31@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1
- **SC\_PRIMARY\_SNAPSHOT\_NAMES** gibt die Namen der primären Snapshots an, die während der Sicherung erstellt wurden.

Beispiele:

- Für einzelne Datenbankinstanz: RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1
  - Für mehrere Datenbankinstanzen: NFSB32@RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1|NFSB31@RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1
  - Für Konsistenzgruppen-Snapshots, die 2 Volumes umfassen: cg3\_R80404CBEF5V1\_04-05-2021\_03.08.03.4945\_0\_bfc279cc-28ad-465c-9d60-5487ac17b25d\_2021\_4\_5\_3\_8\_58\_350
- **SC\_PRIMARY\_MOUNT\_POINTS** gibt die Mount-Point-Details an, die Teil der Sicherung sind.

Die Details umfassen das Verzeichnis, in dem die Volumes bereitgestellt werden, und nicht das unmittelbar übergeordnete Verzeichnis der zu sichernden Datei. Bei einer ASM-Konfiguration ist dies der Name der Datenträgergruppe.

Die Daten werden als <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2> formatiert.

Beispiele:

- Für eine einzelne Datenbankinstanz: /mnt/nfsdb3\_data,/mnt/nfsdb3\_log,/mnt/nfsdb3\_data1
  - Für mehrere Datenbankinstanzen:  
NFSB31@/mnt/nfsdb31\_data,/mnt/nfsdb31\_log,/mnt/nfsdb31\_data1|NFSB32@/mnt/nfsdb32\_data,/mnt/nfsdb32\_log,/mnt/nfsdb32\_data1
  - Für ASM: +DATA2DG,+LOG2DG
- **SC\_PRIMARY\_SNAPSHOTS\_AND\_MOUNT\_POINTS** gibt die Namen der Snapshots an, die während der Sicherung der einzelnen Mount-Punkte erstellt wurden.

Beispiele:

- Für einzelne Datenbankinstanz: RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0:/mnt/nfsb32\_data,RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1:/mnt/nfsb31\_log
- Für mehrere Datenbankinstanzen: NFSB32@RG2\_scspr2417819002\_07-21-

2021\_02.28.26.3973\_0:/mnt/nfsb32\_data,RG2\_scspr2417819002\_07-21-  
2021\_02.28.26.3973\_1:/mnt/nfsb31\_log|NFSB31@RG2\_scspr2417819002\_07-21-  
2021\_02.28.26.3973\_0:/mnt/nfsb31\_data,RG2\_scspr2417819002\_07-21-  
2021\_02.28.26.3973\_1:/mnt/nfsb32\_log

- **SC\_ARCHIVELOGS\_LOCATIONS** gibt den Speicherort des Archivprotokollverzeichnisses an.

Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Archivprotokolldateien. Wenn die Archivprotokolle an mehr als einem Ort abgelegt werden, werden alle Orte erfasst. Hierzu zählen auch die FRA-Szenarien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

Beispiele:

- Für einzelne Datenbank auf NFS: /mnt/nfsdb2\_log
- Für mehrere Datenbanken auf NFS und für die NFSB31-Datenbankarchivprotokolle, die an zwei verschiedenen Orten abgelegt werden:  
NFSB31@/mnt/nfsdb31\_log1,/mnt/nfsdb31\_log2|NFSB32@/mnt/nfsdb32\_log
- Für ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021\_07\_15

- **SC\_REDO\_LOGS\_LOCATIONS** gibt den Speicherort des Redo-Log-Verzeichnisses an.

Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Redo-Logdateien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

Beispiele:

- Für eine einzelne Datenbank auf NFS: /mnt/nfsdb2\_data/newdb1
- Für mehrere Datenbanken auf NFS:  
NFSB31@/mnt/nfsdb31\_data/newdb31|NFSB32@/mnt/nfsdb32\_data/newdb32
- Für ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC\_CONTROL\_FILES\_LOCATIONS** gibt den Speicherort des Steuerdateiverzeichnisses an.

Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Steuerdateien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

Beispiele:

- Für einzelne Datenbanken auf NFS: /mnt/nfsdb2\_data/fra/newdb1,/mnt/nfsdb2\_data/newdb1
- Für mehrere Datenbanken auf NFS:  
NFSB31@/mnt/nfsdb31\_data/fra/newdb31,/mnt/nfsdb31\_data/newdb31|NFSB32@/mnt/nfsdb32\_data/fra/newdb32,/mnt/nfsdb32\_data/newdb32
- Für ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC\_DATA\_FILES\_LOCATIONS"** gibt den Speicherort des Datendateiverzeichnisses an.

Die Verzeichnisnamen sind die unmittelbar übergeordneten Verzeichnisse der Datendateien. Wenn Softlinks für das Verzeichnis verwendet werden, werden diese ausgefüllt.

Beispiele:

- Für einzelne Datenbanken auf NFS: /mnt/nfsdb3\_data1,/mnt/nfsdb3\_data/NEWDB3/datafile
- Für mehrere Datenbanken auf NFS:  
NFSB31@/mnt/nfsdb31\_data1,/mnt/nfsdb31\_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32\_data1,/

mnt/nfsdb32\_data/NEWDB32/datafile

- Für ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE

- **SC\_SNAPSHOT\_LABEL** gibt den Namen der sekundären Beschriftungen an.

Beispiele: Stündlich, Täglich, Wöchentlich, Monatlich oder benutzerdefiniertes Etikett.

#### Unterstützte Trennzeichen

- **:** wird verwendet, um SVM-Name und Volume-Name zu trennen

Beispiel: buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1

- **@** wird verwendet, um Daten von ihrem Datenbanknamen und den Wert von seinem Schlüssel zu trennen.

Beispiele:

- NFSB32@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1
- |NFSB31@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1
- NFSB31@oracle|NFSB32@oracle

- **|** wird verwendet, um die Daten zwischen zwei verschiedenen Datenbanken zu trennen und um die Daten zwischen zwei verschiedenen Entitäten für die Parameter SC\_BACKUP\_ID, SC\_BACKUP\_RETENTION und SC\_BACKUP\_NAME zu trennen.

Beispiele:

- DATEN@203|LOG@205
- Stündlich|DATEN@TAGE:3|LOG@ANZAHL:4
- DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1

- **/** wird verwendet, um den Volumenamen von seinem Snapshot für die Parameter SC\_PRIMARY\_SNAPSHOT\_NAMES und SC\_PRIMARY\_FULL\_SNAPSHOT\_NAME\_FOR\_TAG zu trennen.

Beispiel: NFSB32@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1

- **,** wird verwendet, um Variablensätze für dieselbe Datenbank zu trennen.

Beispiel: NFSB32@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1

|NFSB31@buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_DATA/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scspr2417819002\_NFS\_CDB\_NFSB31\_REDO/RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_1

## Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.



Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

## Sicherungszeitpläne

Die Sicherungshäufigkeit (Zeitplantyp) wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen. Beispielsweise können regelmäßige Sicherungen des Transaktionsprotokolls ausreichen, um sicherzustellen, dass Sie über die erforderlichen Sicherungen verfügen. Je häufiger Sie Ihre Datenbanken sichern, desto weniger Transaktionsprotokolle muss SnapCenter zum Zeitpunkt der Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können als Sicherungshäufigkeit für die

Richtlinie stündlich, täglich, wöchentlich oder monatlich auswählen. Wenn Sie keine dieser Frequenzen auswählen, handelt es sich bei der erstellten Richtlinie um eine Nur-On-Demand-Richtlinie. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

## Namenskonventionen für Backups

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

`resourcegroupname_hostname_timestamp`

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: `customtext_resourcegroup_policy_hostname` oder `resourcegroup_hostname`. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

## Voraussetzungen für die Sicherung einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank sichern, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten



Storage Virtual Machine (SVM) zugewiesen haben.

- Sie sollten überprüft haben, dass alle zur Datenbank gehörenden Datenvolumes und Archivprotokollvolumes geschützt sind, wenn für diese Datenbank der sekundäre Schutz aktiviert ist.
- Sie sollten überprüft haben, dass sich die Datenbank mit Dateien auf den ASM-Datenträgergruppen entweder im Status „MOUNT“ oder „OPEN“ befindet, um ihre Sicherungen mit dem Oracle-Dienstprogramm DBVERIFY zu überprüfen.
- Sie sollten überprüft haben, dass die Länge des Volume-Mount-Punkts 240 Zeichen nicht überschreitet.
- Sie sollten den RESTTimeout-Wert in der Datei *C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config* im SnapCenter Server-Host auf 86400000 ms erhöhen, wenn die zu sichernde Datenbank groß ist (Größe in TB).

Stellen Sie beim Ändern der Werte sicher, dass keine Jobs ausgeführt werden, und starten Sie den SnapCenter SMCore-Dienst nach dem Erhöhen des Werts neu.

## Entdecken Sie für die Sicherung verfügbare Oracle-Datenbanken

Ressourcen sind Oracle-Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Sie können diese Datenbanken zu Ressourcengruppen hinzufügen, um Datenschutzzvorgänge durchzuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

### Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Wenn sich die Datenbanken 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"](#).

- Wenn sich Datenbanken auf einem VMDK-Dateisystem befinden, müssen Sie sich bei vCenter angemeldet und zu **VM-Optionen > Erweitert > Konfiguration bearbeiten** navigiert haben, um den Wert von *disk.enableUUID* für die VM auf „true“ zu setzen.
- Sie müssen den Prozess überprüft haben, dem SnapCenter folgt, um verschiedene Typen und Versionen von Oracle-Datenbanken zu erkennen.

### Schritt 1: Verhindern, dass SnapCenter Einträge erkennt, die nicht in der Datenbank enthalten sind

Sie können verhindern, dass SnapCenter in der oratab-Datei hinzugefügte Einträge erkennt, die nicht zur Datenbank gehören.

#### Schritte

1. Nach der Installation des Plug-Ins für Oracle sollte der Root-Benutzer die Datei **sc\_oratab.config** im Verzeichnis */var/opt/snapcenter/sco/etc/* erstellen.

Erteilen Sie dem Oracle-Binärbesitzer und der Gruppe die Schreibberechtigung, damit die Datei in Zukunft verwaltet werden kann.

2. Der Datenbankadministrator sollte die Nicht-Datenbankeinträge in der Datei **sc\_oratab.config** hinzufügen.

Es wird empfohlen, dasselbe Format beizubehalten, das für die Nicht-Datenbankeinträge in der Datei `/etc/oratab` definiert ist. Alternativ kann der Benutzer einfach die Nicht-Datenbank-Entitätszeichenfolge hinzufügen.



Bei der Zeichenfolge wird zwischen Groß- und Kleinschreibung unterschieden. Jeder Text mit # am Anfang wird als Kommentar behandelt. Der Kommentar kann nach dem Nicht-Datenbanknamen angehängt werden.

For example:

```
-----  
# Sample entries  
# Each line can have only one non-database name  
# These are non-database name  
oratar  # Added by the admin group -1  
#Added by the script team  
NEWSPT  
DBAGNT:/ora01/app/oracle/product/agent:N  
-----
```

### 3. Entdecken Sie die Ressourcen.

Die in `sc_oratab.config` hinzugefügten Nicht-Datenbankeinträge werden nicht auf der Ressourcenseite aufgeführt.



Es wird immer empfohlen, vor dem Upgrade des SnapCenter -Plug-Ins eine Sicherungskopie der Datei `sc_oratab.config` zu erstellen.

## Schritt 2: Ressourcen entdecken

Nach der Installation des Plug-Ins werden alle Datenbanken auf diesem Host automatisch erkannt und auf der Ressourcenseite angezeigt.

Damit die Erkennung der Datenbanken erfolgreich ist, sollten sich die Datenbanken mindestens im gemounteten Zustand oder höher befinden. In einer Oracle Real Application Clusters (RAC)-Umgebung muss sich die RAC-Datenbankinstanz auf dem Host, auf dem die Erkennung durchgeführt wird, mindestens im gemounteten Zustand oder höher befinden, damit die Erkennung der Datenbankinstanz erfolgreich ist. Nur die erfolgreich erkannten Datenbanken können den Ressourcengruppen hinzugefügt werden.

Wenn Sie eine Oracle-Datenbank auf dem Host gelöscht haben, wird SnapCenter Server dies nicht bemerken und die gelöschte Datenbank auflisten. Sie sollten die Ressourcen manuell aktualisieren, um die SnapCenter Ressourcenliste 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“ in der Liste „Ansicht“ die Option „Datenbank“ aus.

Klicken  Filtersymbol] und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern. Sie können dann auf das Symbol `imagfilter_icon.gif` `[Filtersymbol]_icon.png`] klicken,

um den Filterbereich zu schließen.

### 3. Klicken Sie auf **Ressourcen aktualisieren**.

In einem RAC One Node-Szenario wird die Datenbank als RAC-Datenbank auf dem Knoten erkannt, auf dem sie derzeit gehostet wird.

## Ergebnisse

Die Datenbanken werden zusammen mit Informationen wie Datenbanktyp, Host- oder Clusternamen, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

- Wenn sich die Datenbank auf einem Nicht- NetApp -Speichersystem befindet, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ die Meldung „Nicht für Sicherung verfügbar“ an.

Sie können keine Datenschutzvorgänge für die Datenbank durchführen, die sich auf einem Nicht- NetApp -Speichersystem befindet.

- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und nicht geschützt ist, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ die Meldung „Nicht geschützt“ an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ die Meldung „Für Sicherung verfügbar“ an.



Wenn Sie eine Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ressourcenansicht ein rotes Vorhängeschlosssymbol angezeigt. Sie müssen Datenbankmeldeinformationen konfigurieren, um die Datenbank schützen zu können, oder sie der Ressourcengruppe hinzufügen, um Datenschutzvorgänge durchzuführen.

## Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken

Bevor Sie SnapCenter zum Sichern von Oracle-Datenbankressourcen 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 Sicherungstypeneinstellungen angeben. Das Erstellen einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressource oder Ressourcengruppe wiederverwenden möchten.

### Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.
- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erkennen von Datenbanken 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.
- Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen

für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

- 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

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 **Oracle-Datenbank** aus der Dropdown-Liste.
4. Klicken Sie auf **Neu**.
5. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
6. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:

a. Wählen Sie Ihren Speichertyp aus.

b. Wählen Sie den Richtlinienbereich aus:

- Wenn Sie **ein Online-Backup erstellen** möchten, wählen Sie **Online-Backup**.

Sie müssen angeben, ob Sie alle Datendateien, Steuerdateien und Archivprotokolldateien, nur Datendateien und Steuerdateien oder nur Archivprotokolldateien sichern möchten.

- Wenn Sie **eine Offline-Sicherung erstellen** möchten, wählen Sie **Offline-Sicherung** und dann eine der folgenden Optionen:

- Wenn Sie eine Offlinesicherung erstellen möchten, während sich die Datenbank im gemounteten Zustand befindet, wählen Sie **Mount**.
- Wenn Sie eine Offline-Shutdown-Sicherung erstellen möchten, indem Sie die Datenbank in den Shutdown-Status versetzen, wählen Sie **Shutdown**.

Wenn Sie über Pluggable Databases (PDBs) verfügen und den Status der PDBs vor dem Erstellen der Sicherung speichern möchten, müssen Sie **Status der PDBs speichern** auswählen. Dadurch können Sie die PDBs nach der Erstellung des Backups in ihren ursprünglichen Zustand zurückversetzen.

- c. Wenn Sie die Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren**.

Sie können die verzögerte Katalogisierung für jeweils eine Sicherung entweder über die GUI oder über den SnapCenter -CLI-Befehl `Catalog-SmBackupWithOracleRMAN` durchführen.



Wenn Sie Sicherungen einer RAC-Datenbank katalogisieren möchten, stellen Sie sicher, dass für diese Datenbank kein anderer Job ausgeführt wird. Wenn ein anderer Job ausgeführt wird, schlägt der Katalogisierungsvorgang fehl, anstatt in die Warteschlange gestellt zu werden.

d. Wenn Sie Archivprotokolle nach der Sicherung bereinigen möchten, wählen Sie **Archivprotokolle nach der Sicherung bereinigen**.



Das Bereinigen von Archivprotokollen aus dem Archivprotokollziel, das in der Datenbank nicht konfiguriert ist, wird übersprungen.



Wenn Sie Oracle Standard Edition verwenden, können Sie beim Durchführen einer Archivprotokollsicherung die Parameter LOG\_ARCHIVE\_DEST und LOG\_ARCHIVE\_DUPLEX\_DEST verwenden.

- Sie können Archivprotokolle nur löschen, wenn Sie die Archivprotokolldateien als Teil Ihrer Sicherung ausgewählt haben.



Sie müssen sicherstellen, dass alle Knoten in einer RAC-Umgebung auf alle Archivprotokollspeicherorte zugreifen können, damit der Löschvorgang erfolgreich ist.

| Wenn Sie wollen...                                                                    | Dann...                                                                                                                                                 |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alle Archivprotokolle löschen                                                         | Wählen Sie <b>Alle Archivprotokolle löschen</b> .                                                                                                       |
| Löschen Sie ältere Archivprotokolle                                                   | Wählen Sie <b>Archivprotokolle löschen, die älter sind als</b> und geben Sie dann das Alter der zu löschenden Archivprotokolle in Tagen und Stunden an. |
| Archivprotokolle von allen Zielen löschen                                             | Wählen Sie <b>Archivprotokolle von allen Zielen löschen</b> .                                                                                           |
| Löschen Sie die Archivprotokolle aus den Protokollzielen, die Teil der Sicherung sind | Wählen Sie <b>Archivprotokolle aus den Zielen löschen, die Teil der Sicherung sind</b> .                                                                |

+

☒ Prune archive logs after backup

**Prune log retention setting**

☐ Delete all archive logs

☒ Delete archive logs older than

**Prune log destination setting**

☐ Delete archive logs from all the destinations

☒ Delete archive logs from the destinations which are part of backup

7. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:

- a. Geben Sie die Zeitplanhäufigkeit an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum und Enddatum) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- a. Geben Sie im Abschnitt „Einstellungen für die Aufbewahrung von Daten-Snapshots“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

| Wenn Sie wollen...                               | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Snapshots | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> <div>  <p>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.</p> </div> <div>  <p>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.</p> </div> |

|                                                                    |                                                                                                                                                                                                               |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.                                                 |
| Sperrzeitraum für Snapshot-Kopien                                  | <p>Wählen Sie den <b>Sperrzeitraum für die Snapshot-Kopie</b> und geben Sie die Dauer in Tagen, Monaten oder Jahren an.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p> |

- b. Geben Sie im Abschnitt „Aufbewahrungseinstellungen für Archivprotokoll-Snapshots“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

| Wenn Sie wollen...                               | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Snapshots | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> <div>  <p>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.</p> </div> <div>  <p>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.</p> </div> |

|                                                                    |                                                                                                                                                                                                               |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.                                                 |
| Sperrzeitraum für Snapshot-Kopien                                  | <p>Wählen Sie den <b>Sperrzeitraum für die Snapshot-Kopie</b> und geben Sie die Dauer in Tagen, Monaten oder Jahren an.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p> |

c. 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.

8. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:



Sie müssen die sekundären Replikationsoptionen für den **Sperrzeitraum für sekundäre Snapshot-Kopien** auswählen, damit diese wirksam werden.

| Für dieses Feld...                                                      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots | <p>Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation).</p> <p>Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> |



| Für dieses Feld...                                                     | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots | <p>Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).</p> <p>Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.</p> <p>Weitere Informationen zu SnapLock Vault finden Sie unter <a href="#">"Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel"</a></p> <p>Sehen <a href="#">"Anzeigen von Oracle-Datenbanksicherungen und -klonen auf der Seite „Topologie“"</a> .</p> |
| Fehleranzahl der Wiederholungsversuche                                 | Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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 müssen die Prescripts und Postscripts entweder in `/var/opt/snapcenter/spl/scripts` oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad `/var/opt/snapcenter/spl/scripts` ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

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

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen. ["Mehr erfahren"](#)

10. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

- a. Wählen Sie den Sicherungszeitplan aus, für den Sie den Überprüfungsvorgang durchführen möchten.
- b. Geben Sie im Abschnitt „Befehle des Überprüfungsskripts“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das Sie vor bzw. nach dem Überprüfungsvorgang ausführen möchten.

Sie müssen die Prescripts und Postscripts entweder in `/var/opt/snapcenter/spl/scripts` oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad `/var/opt/snapcenter/spl/scripts` ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

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

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

## Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Oracle-Datenbanken hinzu

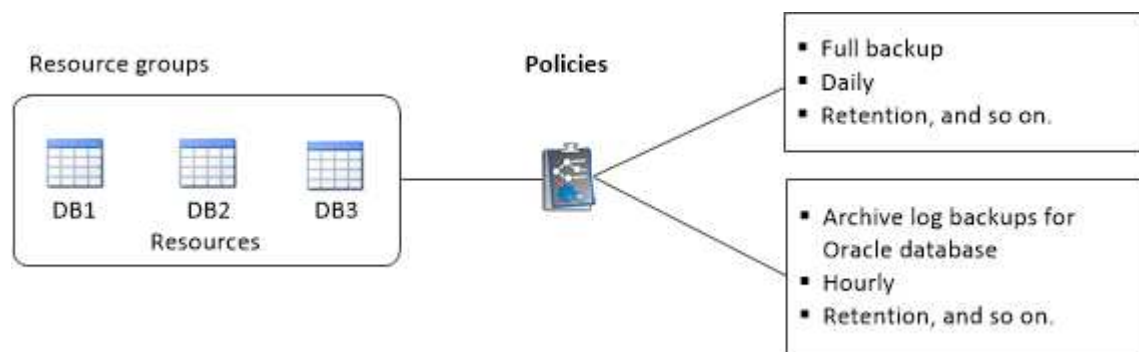
Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern.

### 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 Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken 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 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 Oracle festgelegt wurde, einschließlich Präfix, falls erforderlich.

4. Wählen Sie auf der Seite „Ressourcen“ einen Oracle-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 Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.



Sie können Datenbanken von Linux- und AIX-Hosts in einer einzigen Ressourcengruppe hinzufügen.

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 *Richtliniennamen*“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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. 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                                                                         |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> .                                                        |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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.

9. 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-SmSmtServer“ angegeben haben.

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

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Oracle-Ressourcen 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 *Richtliniennamenname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamenname* 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“ (Richtliniennamenname) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                  |
|------------------------------------------------------|----------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> . |

| Wenn Sie wollen...          | Machen Sie Folgendes...                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Planen Sie eine Überprüfung | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Sichern von Oracle-Ressourcen

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 „Datenbank“ aus.
3. Klicken  und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern.

Sie können dann auf , um den Filterbereich zu schließen.

4. Wählen Sie die Datenbank aus, die Sie sichern möchten.

Die Seite „Datenbank schützen“ wird angezeigt.

5. Führen Sie auf der Seite „Ressourcen“ die folgenden Schritte aus:
  - 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.

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

6. 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 *Richtliniennamenname* 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.

7. 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 den sekundären Speicher zu überprüfen.
- b. Klicken  in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren. + Im Dialogfeld „Verifizierungszeitpläne hinzufügen *Richtliniennamenname*“ können Sie die folgenden Schritte ausführen:
- c. Wählen Sie **Überprüfung nach Sicherung ausführen**.
- d. Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie den Zeitplantyp aus der Dropdownliste aus.



In einem Flex ASM-Setup können Sie keine Überprüfungsvorgänge an Blattknoten durchführen, wenn die Kardinalität kleiner ist als die Anzahl der Knoten im RAC-Cluster.

- e. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Backups auf dem sekundären Speicher zu überprüfen.
- f. Klicken Sie auf **OK**.

Die konfigurierten Überprüfungszeitpläne 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-SmSmtServer` .

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

Die Seite „Datenbanktopologie“ 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.

### Nach Abschluss

- Im AIX-Setup können Sie die `lkdev` Befehl zum Sperren und die `rendev` Befehl zum Umbenennen der Datenträger, auf denen sich die gesicherte Datenbank befand.

Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mithilfe dieser Sicherung durchführen.

- Wenn der Sicherungsvorgang fehlschlägt, weil die Ausführungszeit der Datenbankabfrage den Timeout-Wert überschritten hat, sollten Sie den Wert der Parameter `ORACLE_SQL_QUERY_TIMEOUT` und `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` ändern, indem Sie den `Set-SmConfigSettings` Cmdlet:

Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter Plug-in Loader (SPL)-Dienst neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Wenn während des Überprüfungsprozesses nicht auf die Datei zugegriffen werden kann und der Einhängpunkt nicht verfügbar ist, schlägt der Vorgang möglicherweise mit dem Fehlercode DBV-00100 für die angegebene Datei fehl. Sie sollten die Werte der Parameter `VERIFICATION_DELAY` und `VERIFICATION_RETRY_COUNT` in `sco.properties` ändern.

Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter Plug-in Loader (SPL)-Dienst neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.
- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl.

Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`.

### Weitere Informationen

- ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)
- ["Die Oracle RAC One Node-Datenbank wird für die Durchführung von SnapCenter -Vorgängen übersprungen"](#)
- ["Der Status einer Oracle 12c ASM-Datenbank konnte nicht geändert werden"](#)

- "Anpassbare Parameter für Sicherungs-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"(Anmeldung erforderlich)

## Sichern von Oracle-Datenbankressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Der Sicherungsvorgang wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

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.



Wenn Sie über eine föderierte Ressourcengruppe mit zwei Datenbanken verfügen und eine davon Daten auf einem Nicht- NetApp -Speicher enthält, wird der Sicherungsvorgang abgebrochen, obwohl sich die andere Datenbank auf einem NetApp -Speicher befindet.

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.

### Nach Abschluss

- Im AIX-Setup können Sie die `lkdev` Befehl zum Sperren und die `rendev` Befehl zum Umbenennen der Datenträger, auf denen sich die gesicherte Datenbank befand.

Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mithilfe dieser Sicherung durchführen.

- Wenn der Sicherungsvorgang fehlschlägt, weil die Ausführungszeit der Datenbankabfrage den Timeout-Wert überschritten hat, sollten Sie den Wert der Parameter `ORACLE_SQL_QUERY_TIMEOUT` und `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` ändern, indem Sie den `Set-SmConfigSettings` Cmdlet:

Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter Plug-in Loader (SPL)-Dienst neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl`

restart

- Wenn während des Überprüfungsprozesses nicht auf die Datei zugegriffen werden kann und der Einhängpunkt nicht verfügbar ist, schlägt der Vorgang möglicherweise mit dem Fehlercode DBV-00100 für die angegebene Datei fehl. Sie sollten die Werte der Parameter VERIFICATION\_DELAY\_ und VERIFICATION\_RETRY\_COUNT in sco.properties ändern.

Nachdem Sie den Wert der Parameter geändert haben, starten Sie den SnapCenter Plug-in Loader (SPL)-Dienst neu, indem Sie den folgenden Befehl ausführen /opt/NetApp/snapcenter/spl/bin/spl

restart

## Überwachen der Oracle-Datenbanksicherung

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

### Überwachen von Oracle-Datenbanksicherungsvorgängen

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.

## Andere Sicherungsvorgänge

### Sichern Sie Oracle-Datenbanken mit UNIX-Befehlen

Der Sicherungsworkflow umfasst die Planung, die Identifizierung der Ressourcen für die Sicherung, die Erstellung von Sicherungsrichtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Sicherungen und die Überwachung der Vorgänge.

### Was Sie brauchen

- Sie sollten die Speichersystemverbindungen hinzugefügt und die Anmeldeinformationen mit den Befehlen *Add-SmStorageConnection* und *Add-SmCredential* erstellt haben.
- Sie sollten die Verbindungssitzung mit dem SnapCenter -Server mit dem Befehl *Open-SmConnection* hergestellt haben.

Sie können nur eine Anmeldesitzung für das SnapCenter -Konto haben und das Token wird im Home-Verzeichnis des Benutzers gespeichert.



Die Verbindungssitzung ist nur 24 Stunden gültig. Sie können jedoch mit der Option „TokenNeverExpires“ ein Token erstellen, das nie abläuft und die Sitzung immer gültig ist.

## Über diese Aufgabe

Sie sollten die folgenden Befehle ausführen, um die Verbindung mit dem SnapCenter -Server herzustellen, die

Oracle-Datenbankinstanzen zu ermitteln, Richtlinien und Ressourcengruppen hinzuzufügen, eine Sicherung durchzuführen und die Sicherung zu überprüfen.

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](#)".

## Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer: *Open-SmConnection*
2. Führen Sie den Vorgang zur Erkennung von Hostressourcen durch: *Get-SmResources*
3. Konfigurieren Sie die Anmeldeinformationen und bevorzugten Knoten der Oracle-Datenbank für den Sicherungsvorgang einer Real Application Cluster (RAC)-Datenbank: *Configure-SmOracleDatabase*
4. Erstellen Sie eine Sicherungsrichtlinie: *Add-SmPolicy*
5. Rufen Sie die Informationen zum sekundären Speicherort (SnapVault oder SnapMirror) ab: *Get-SmSecondaryDetails*

Dieser Befehl ruft die Zuordnungsdetails zwischen Primär- und Sekundärspeicher einer angegebenen Ressource ab. Sie können die Zuordnungsdetails verwenden, um die sekundären Überprüfungseinstellungen beim Erstellen einer Sicherungsressourcengruppe zu konfigurieren.

6. Fügen Sie SnapCenter eine Ressourcengruppe hinzu: *Add-SmResourceGroup*
7. Erstellen Sie ein Backup: *New-SmBackup*

Sie können den Job mit der Option „WaitForCompletion“ abfragen. Wenn diese Option angegeben ist, fragt der Befehl den Server weiterhin ab, bis der Sicherungsauftrag abgeschlossen ist.

8. Rufen Sie die Protokolle von SnapCenter ab: *Get-SmLogs*

## Abbrechen von Sicherungsvorgängen von Oracle-Datenbanken

Sie können Sicherungsvorgänge abbrechen, die entweder ausgeführt werden, in der Warteschlange stehen oder nicht reagieren.

Sie müssen als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Sicherungsvorgänge abzubrechen.

### Über diese Aufgabe

Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter Server den Vorgang und entfernt alle Snapshots aus dem Speicher, wenn die erstellte Sicherung nicht beim SnapCenter -Server registriert ist. Wenn die Sicherung bereits beim SnapCenter Server registriert ist, wird der bereits erstellte Snapshot auch nach dem Auslösen des Abbruchs nicht zurückgesetzt.

- Sie können nur Protokoll- oder vollständige Sicherungsvorgänge abbrechen, die sich in der Warteschlange befinden oder ausgeführt werden.
- Sie können den Vorgang nicht mehr abbrechen, nachdem die Überprüfung begonnen hat.

Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Überprüfungsvorgang wird nicht durchgeführt.

- Sie können den Sicherungsvorgang nicht abbrechen, nachdem die Katalogvorgänge gestartet wurden.
- Sie können einen Sicherungsvorgang entweder auf der Seite „Überwachen“ oder im Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter -GUI können Sie CLI-Befehle verwenden, um Vorgänge abzuberechnen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

## Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"> <li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li> <li>2. Wählen Sie den Vorgang aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li> </ol>                                                                                                                                                                              |
| Aktivitätsbereich | <ol style="list-style-type: none"> <li>1. Klicken Sie nach dem Starten des Sicherungsauftrags auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li> <li>2. Wählen Sie den Vorgang aus.</li> <li>3. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li> </ol> |

## Ergebnisse

Der Vorgang wird abgebrochen und die Ressource in den ursprünglichen Zustand zurückversetzt.

Wenn der von Ihnen abgebrochene Vorgang im Status „Abbrechen“ oder „Ausführen“ nicht reagiert, sollten Sie „Cancel-SmJob -JobID <int> -Force“ ausführen, um den Sicherungsvorgang zwangsweise zu beenden.

## Anzeigen von Oracle-Datenbanksicherungen und -klonen auf der Seite „Topologie“

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

## Über diese Aufgabe

Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen 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 sowie die Gesamtzahl der Protokollsicherungen 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 die Anwendungsressource auf 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 Vorgänge wie Wiederherstellen, Klonen, Mounten, Unmounten, Umbenennen, Katalogisieren, Dekatalogisieren und Löschen durchzuführen.



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

- Wenn Sie eine Protokollsicherung ausgewählt haben, können Sie nur die Vorgänge Umbenennen, Einbinden, Aufheben der Einbindung, Katalogisieren, Auskatalogisieren und Löschen durchführen.
  - Wenn Sie die Sicherung mit Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Sicherungen nicht umbenennen.
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

Wenn der SnapmirrorStatusUpdateWaitTime zugewiesene Wert kleiner ist, werden die Mirror- und Vault-Sicherungskopien nicht auf der Topologieseite aufgeführt, selbst wenn Daten- und Protokollvolumes erfolgreich geschützt wurden. Sie sollten den SnapmirrorStatusUpdateWaitTime zugewiesenen Wert mithilfe des PowerShell-Cmdlets *Set-SmConfigSettings* erhöhen.

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](#)" oder "[Referenzhandbuch für SnapCenter -Software-Cmdlets](#)" .



# Mounten und Unmounten von Datenbanksicherungen

Sie können einzelne oder mehrere Daten bereitstellen und nur Backups protokollieren, wenn Sie auf die Dateien im Backup zugreifen möchten. Sie können das Backup entweder auf demselben Host mounten, auf dem das Backup erstellt wurde, oder auf einem Remote-Host mit demselben Oracle- und Host-Konfigurationstyp. Wenn Sie die Sicherungen manuell bereitgestellt haben, sollten Sie die Bereitstellung der Sicherungen nach Abschluss des Vorgangs manuell aufheben. Zu jedem beliebigen Zeitpunkt kann eine Sicherungskopie einer Datenbank auf einem beliebigen Host bereitgestellt werden. Während der Ausführung eines Vorgangs können Sie nur eine einzige Sicherung mounten.



In einem Flex ASM-Setup können Sie keine Mount-Operationen auf Leaf-Knoten durchführen, wenn die Kardinalität kleiner ist als die Anzahl der Knoten im RAC-Cluster.

## Mounten einer Datenbanksicherung

Sie sollten eine Datenbanksicherung manuell mounten, wenn Sie auf die Dateien in der Sicherung zugreifen möchten.

### Was Sie brauchen

- Wenn Sie über eine Automatic Storage Management (ASM)-Datenbankinstanz in einer NFS-Umgebung verfügen und die ASM-Sicherungen mounten möchten, sollten Sie den ASM-Festplattenpfad `/var/opt/snapcenter/sco/backup*/*/*/*` zum vorhandenen Pfad hinzugefügt haben, der im Parameter `asm_diskstring` definiert ist.
- Wenn Sie über eine ASM-Datenbankinstanz in einer NFS-Umgebung verfügen und die ASM-Protokollsicherungen als Teil eines Wiederherstellungsvorgangs bereitstellen möchten, sollten Sie den ASM-Festplattenpfad `/var/opt/snapcenter/scu/clones/*/*_` zum vorhandenen Pfad hinzugefügt haben, der im Parameter `asm_diskstring` definiert ist.
- Im Parameter `asm_diskstring` sollten Sie `AFD:*` konfigurieren, wenn Sie ASMFD verwenden, oder `ORCL:*`, wenn Sie ASMLIB verwenden.



Informationen zum Bearbeiten des Parameters `asm_diskstring` finden Sie unter ["So fügen Sie Datenträgerpfade zu `asm\_diskstring` hinzu"](#).

- Sie sollten die ASM-Anmeldeinformationen und den ASM-Port konfigurieren, wenn diese beim Mounten der Sicherung von denen des Quelldatenbankhosts abweichen.
- Wenn Sie einen alternativen Host mounten möchten, müssen Sie überprüfen, ob der alternative Host die folgenden Anforderungen erfüllt:
  - Dieselbe UID und GID wie die des ursprünglichen Hosts
  - Dieselbe Oracle-Version wie die des ursprünglichen Hosts
  - Dieselbe Betriebssystemverteilung und -version wie die des ursprünglichen Hosts
  - Für NVMe sollte NVMe util installiert sein
- Sie sollten sicherstellen, dass die LUN nicht mithilfe einer iGroup, die aus gemischten Protokollen iSCSI und FC besteht, auf den AIX-Host abgebildet wird. Weitere Informationen finden Sie unter ["Der Vorgang schlägt mit dem Fehler „Gerät für LUN konnte nicht erkannt werden“ fehl."](#)

## 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank entweder aus der Datenbankdetailansicht oder aus der Ressourcengruppendedetailansicht aus.

Die Seite „Datenbanktopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder vom primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.

5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf  .

6. Wählen Sie auf der Seite „Backups mounten“ aus der Dropdown-Liste **Wählen Sie den Host zum Mounten des Backups** den Host aus, auf dem Sie das Backup mounten möchten.

Der Mount-Pfad `/var/opt/snapcenter/sco/backup_mount/backup_name/database_name` wird angezeigt.

Wenn Sie die Sicherung einer ASM-Datenbank mounten, wird der Mount-Pfad `+diskgroupname_SID_backupid` angezeigt.

7. Klicken Sie auf **Mounten**.

## Nachdem Sie fertig sind

- Sie können den folgenden Befehl ausführen, um die Informationen zum bereitgestellten Backup abzurufen:

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- Wenn Sie eine ASM-Datenbank gemountet haben, können Sie den folgenden Befehl ausführen, um die Informationen zum gemounteten Backup abzurufen:

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- Um die Sicherungs-ID abzurufen, führen Sie den folgenden Befehl aus:

```
./sccli Get-Smbbackup-BackupNamebackup_name
```

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"](#) .

## Unmounten einer Datenbanksicherung

Sie können die Bereitstellung einer bereitgestellten Datenbanksicherung manuell aufheben, wenn Sie nicht mehr auf die Dateien in der Sicherung zugreifen 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank entweder aus der Datenbankdetailansicht oder aus der Ressourcengruppendetailansicht aus.

Die Seite „Datenbanktopologie“ wird angezeigt.

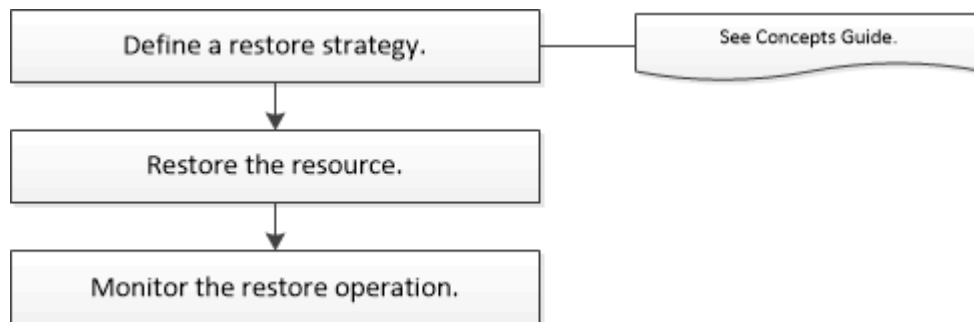
4. Wählen Sie das bereitgestellte Backup aus und klicken Sie dann auf .
5. Klicken Sie auf **OK**.

## Wiederherstellen und Wiederherstellen von Oracle-Datenbanken

### Wiederherstellungs-Workflow

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



### Definieren Sie eine Wiederherstellungsstrategie für Oracle-Datenbanken

Sie müssen vor der Wiederherstellung Ihrer Datenbank eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.

### Für Wiederherstellungsvorgänge unterstützte Sicherungstypen

SnapCenter unterstützt die Wiederherstellung und Wiedergewinnung verschiedener Arten von Oracle-Datenbanksicherungen.

- Online-Datensicherung
- Offline-Shutdown-Datensicherung
- Offline-Mount-Datensicherung



Wenn Sie eine Offline-Shutdown- oder Offline-Mount-Datensicherung wiederherstellen, belässt SnapCenter die Datenbank im Offline-Zustand. Sie sollten die Datenbank manuell wiederherstellen und die Protokolle zurücksetzen.

- Vollständige Sicherung
- Offline-Mount-Backups von Data Guard-Standbydatenbanken
- Reine Daten-Online-Backups von Active Data Guard-Standby-Datenbanken



Sie können keine Wiederherstellung von Active Data Guard-Standbydatenbanken durchführen.

- Online-Datensicherungen, Online-Vollsicherungen, Offline-Mount-Sicherungen und Offline-Shutdown-Sicherungen in einer Real Application Clusters (RAC)-Konfiguration
- Online-Datensicherungen, Online-Vollsicherungen, Offline-Mount-Sicherungen und Offline-Shutdown-Sicherungen in einer Automatic Storage Management (ASM)-Konfiguration

### Für Oracle-Datenbanken unterstützte Wiederherstellungsmethoden

SnapCenter unterstützt Connect-and-Copy oder In-Place-Wiederherstellung für Oracle-Datenbanken. Während eines Wiederherstellungsvorgangs ermittelt SnapCenter die für das Dateisystem geeignete Wiederherstellungsmethode, die für die Wiederherstellung ohne Datenverlust verwendet werden soll.



SnapCenter unterstützt kein volumenbasiertes SnapRestore.

### Verbinden und Kopieren wiederherstellen

Wenn das Datenbanklayout vom Backup abweicht oder nach der Erstellung des Backups neue Dateien vorhanden sind, wird eine Connect-and-Copy-Wiederherstellung durchgeführt. Bei der Wiederherstellungsmethode „Verbinden und Kopieren“ werden die folgenden Aufgaben ausgeführt:

#### Schritte

1. Das Volume wird aus dem Snapshot geklont und der Dateisystemstapel wird mithilfe der geklonten LUNs oder Volumes auf dem Host erstellt.
2. Die Dateien werden von den geklonten Dateisystemen in die ursprünglichen Dateisysteme kopiert.
3. Die geklonten Dateisysteme werden dann vom Host abgemeldet und die geklonten Volumes werden von ONTAP gelöscht.



Für ein Flex ASM-Setup (bei dem die Kardinalität geringer ist als die Anzahl der Knoten im RAC-Cluster) oder ASM RAC-Datenbanken auf VMDK oder RDM wird nur die Wiederherstellungsmethode „Verbinden und Kopieren“ unterstützt.

Auch wenn Sie die direkte Wiederherstellung zwangsweise aktiviert haben, führt SnapCenter in den folgenden Szenarien eine Connect-and-Copy-Wiederherstellung durch:

- Wiederherstellung vom sekundären Speichersystem
- Wiederherstellung von ASM-Datenträgergruppen auf Knoten eines Oracle RAC-Setups, auf dem keine Datenbankinstanz konfiguriert ist
- Im Oracle RAC-Setup auf einem der Peer-Knoten, wenn die ASM-Instanz oder die Cluster-Instanz nicht

ausgeführt wird oder wenn der Peer-Knoten ausgefallen ist

- Nur Wiederherstellung von Steuerdateien
- Stellen Sie eine Teilmenge der Tablespaces wieder her, die sich auf einer ASM-Datenträgergruppe befinden
- Die Datenträgergruppe wird zwischen Datendateien, SP-Dateien und Kennwortdateien gemeinsam genutzt.
- Der SnapCenter Plug-in Loader (SPL)-Dienst ist nicht installiert oder wird auf dem Remote-Knoten in einer RAC-Umgebung nicht ausgeführt
- Dem Oracle RAC werden neue Knoten hinzugefügt, und der SnapCenter Server erkennt die neu hinzugefügten Knoten nicht.

### In-Place-Wiederherstellung

Wenn das Datenbanklayout dem Backup ähnelt und keine Konfigurationsänderungen am Speicher- und Datenbankstapel vorgenommen wurden, wird eine In-Place-Wiederherstellung durchgeführt, wobei die Wiederherstellung der Datei oder LUN auf ONTAP durchgeführt wird. SnapCenter unterstützt nur Single File SnapRestore (SFSR) als Teil der In-Place-Wiederherstellungsmethode.



NetApp ONTAP unterstützt die In-Place-Wiederherstellung vom sekundären Standort.

Wenn Sie eine direkte Wiederherstellung der Datenbank durchführen möchten, stellen Sie sicher, dass sich auf der ASM-Datenträgergruppe nur Datendateien befinden. Sie müssen nach allen Änderungen an der ASM-Datenträgergruppe oder an der physischen Struktur der Datenbank eine Sicherung erstellen. Nach der Durchführung der In-Place-Wiederherstellung enthält die Datenträgergruppe dieselbe Anzahl Datendateien wie zum Zeitpunkt der Sicherung.

Die direkte Wiederherstellung wird automatisch angewendet, wenn die Datenträgergruppe oder der Bereitstellungspunkt die folgenden Kriterien erfüllt:

- Nach der Sicherung werden keine neuen Datendateien hinzugefügt (Fremddateiprüfung)
- Kein Hinzufügen, Löschen oder Neuerstellen von ASM-Datenträgern oder LUNs nach der Sicherung (Prüfung auf strukturelle Änderungen der ASM-Datenträgergruppe)
- Kein Hinzufügen, Löschen oder Neuerstellen von LUNs zur LVM-Datenträgergruppe (Prüfung auf strukturelle Änderungen in der LVM-Datenträgergruppe)



Sie können die In-Place-Wiederherstellung auch zwangsweise aktivieren, indem Sie entweder die GUI, die SnapCenter CLI oder das PowerShell-Cmdlet verwenden, um die Prüfung auf Fremddateien und die Prüfung auf strukturelle Änderungen der LVM-Datenträgergruppe zu überschreiben.

### Durchführen einer In-Place-Wiederherstellung auf ASM RAC

In SnapCenter wird der Knoten, auf dem Sie die Wiederherstellung durchführen, als primärer Knoten bezeichnet und alle anderen Knoten des RAC, auf denen sich die ASM-Datenträgergruppe befindet, werden als Peer-Knoten bezeichnet. SnapCenter ändert den Status der ASM-Datenträgergruppe, um die Bereitstellung auf allen Knoten aufzuheben, auf denen sich die ASM-Datenträgergruppe im Bereitstellungsstatus befindet, bevor der Speicherwiederherstellungsvorgang ausgeführt wird. Nachdem die Speicherwiederherstellung abgeschlossen ist, ändert SnapCenter den Status der ASM-Datenträgergruppe in den Zustand vor dem Wiederherstellungsvorgang.

In SAN-Umgebungen entfernt SnapCenter Geräte von allen Peer-Knoten und führt vor der

Speicherwiederherstellung einen LUN-Unmap-Vorgang durch. Nach der Speicherwiederherstellung führt SnapCenter eine LUN-Zuordnungsoperation durch und erstellt Geräte auf allen Peer-Knoten. Wenn sich das Oracle RAC ASM-Layout in einer SAN-Umgebung auf LUNs befindet, führt SnapCenter während der Wiederherstellung LUN-Unmap-, LUN-Restore- und LUN-Map-Vorgänge auf allen Knoten des RAC-Clusters durch, auf dem sich die ASM-Datenträgergruppe befindet. Auch wenn vor der Wiederherstellung nicht alle Initiatoren der RAC-Knoten für die LUNs verwendet wurden, erstellt SnapCenter nach der Wiederherstellung eine neue iGroup mit allen Initiatoren aller RAC-Knoten.

- Wenn während der Vorwiederherstellungsaktivität auf Peer-Knoten ein Fehler auftritt, setzt SnapCenter den Zustand der ASM-Datenträgergruppe automatisch auf den Zustand zurück, in dem er sich vor der Wiederherstellung auf Peer-Knoten befand, auf denen der Vorwiederherstellungsvorgang erfolgreich war. Ein Rollback wird für den primären Knoten und den Peer-Knoten, auf dem der Vorgang fehlgeschlagen ist, nicht unterstützt. Bevor Sie eine weitere Wiederherstellung versuchen, müssen Sie das Problem auf dem Peer-Knoten manuell beheben und die ASM-Datenträgergruppe auf dem primären Knoten wieder in den Mount-Zustand versetzen.
- Wenn während der Wiederherstellungsaktivität ein Fehler auftritt, schlägt der Wiederherstellungsvorgang fehl und es wird kein Rollback durchgeführt. Bevor Sie eine weitere Wiederherstellung versuchen, müssen Sie das Problem bei der Speicherwiederherstellung manuell beheben und die ASM-Datenträgergruppe auf dem primären Knoten wieder in den Mount-Zustand versetzen.
- Wenn während der Postrestore-Aktivität auf einem der Peer-Knoten ein Fehler auftritt, fährt SnapCenter mit dem Wiederherstellungsvorgang auf den anderen Peer-Knoten fort. Sie müssen das Problem nach der Wiederherstellung auf dem Peer-Knoten manuell beheben.

## **Für Oracle-Datenbanken unterstützte Wiederherstellungsarten**

Mit SnapCenter können Sie verschiedene Arten von Wiederherstellungsvorgängen für Oracle-Datenbanken durchführen.

Vor der Wiederherstellung der Datenbank werden die Sicherungen validiert, um festzustellen, ob im Vergleich zu den tatsächlichen Datenbankdateien Dateien fehlen.

### **Vollständige Wiederherstellung**

- Stellt nur die Datendateien wieder her
- Stellt nur die Steuerdateien wieder her
- Stellt die Datendateien und Steuerdateien wieder her
- Stellt Datendateien, Steuerdateien und Redo-Log-Dateien in Data Guard-Standby- und Active Data Guard-Standby-Datenbanken wieder her

### **Teilweise Wiederherstellung**

- Stellt nur die ausgewählten Tablespaces wieder her
- Stellt nur die ausgewählten Pluggable Databases (PDBs) wieder her
- Stellt nur die ausgewählten Tablespaces einer PDB wieder her

## **Für Oracle-Datenbanken unterstützte Arten von Wiederherstellungsvorgängen**

Mit SnapCenter können Sie verschiedene Arten von Wiederherstellungsvorgängen für Oracle-Datenbanken durchführen.

- Die Datenbank bis zur letzten Transaktion (alle Protokolle)

- Die Datenbank bis zu einer bestimmten Systemänderungsnummer (SCN)
- Die Datenbank bis zu einem bestimmten Datum und einer bestimmten Uhrzeit

Sie müssen Datum und Uhrzeit für die Wiederherstellung basierend auf der Zeitzone des Datenbankhosts angeben.

SnapCenter bietet auch die Option „Keine Wiederherstellung“ für Oracle-Datenbanken.



Das Plug-In für Oracle-Datenbanken unterstützt keine Wiederherstellung, wenn Sie die Wiederherstellung mithilfe einer Sicherung durchgeführt haben, die mit der Datenbankrolle als Standby erstellt wurde. Für physische Standby-Datenbanken müssen Sie immer eine manuelle Wiederherstellung durchführen.

## Einschränkungen im Zusammenhang mit der Wiederherstellung und Wiederherstellung von Oracle-Datenbanken

Bevor Sie Wiederherstellungsvorgänge durchführen, müssen Sie sich der Einschränkungen bewusst sein.

Wenn Sie eine beliebige Version von Oracle zwischen 11.2.0.4 und 12.1.0.1 verwenden, bleibt der Wiederherstellungsvorgang hängen, wenn Sie den Befehl *renamedg* ausführen. Sie können den Oracle-Patch 19544733 anwenden, um dieses Problem zu beheben.

Die folgenden Wiederherstellungsvorgänge werden nicht unterstützt:

- Wiederherstellung und Recovery von Tablespaces der Root-Containerdatenbank (CDB)
- Wiederherstellung temporärer Tablespaces und temporärer Tablespaces, die mit PDBs verknüpft sind
- Wiederherstellung und Recovery von Tablespaces aus mehreren PDBs gleichzeitig
- Wiederherstellung von Protokollsicherungen
- Wiederherstellung von Backups an einem anderen Ort
- Wiederherstellung von Redo-Log-Dateien in jeder Konfiguration außer Data Guard-Standby- oder Active Data Guard-Standby-Datenbanken
- Wiederherstellen der SPFILE- und Kennwortdatei
- Wenn Sie einen Wiederherstellungsvorgang für eine Datenbank durchführen, die mit dem bereits vorhandenen Datenbanknamen auf demselben Host neu erstellt wurde, von SnapCenter verwaltet wurde und über gültige Sicherungen verfügte, überschreibt der Wiederherstellungsvorgang die neu erstellten Datenbankdateien, obwohl die DBIDs unterschiedlich sind.

Dies kann durch Ausführen einer der folgenden Aktionen vermieden werden:

- Entdecken Sie die SnapCenter -Ressourcen, nachdem die Datenbank neu erstellt wurde
- Erstellen Sie eine Sicherungskopie der neu erstellten Datenbank

## Einschränkungen im Zusammenhang mit der Point-in-Time-Wiederherstellung von Tablespaces

- Die zeitpunktbezogene Wiederherstellung (PITR) von SYSTEM-, SYSAUX- und UNDO-Tablespaces wird nicht unterstützt.
- PITR von Tablespaces kann nicht zusammen mit anderen Wiederherstellungsarten durchgeführt werden
- Wenn ein Tablespace umbenannt wird und Sie ihn auf einen Zustand vor der Umbenennung zurücksetzen möchten, sollten Sie den früheren Namen des Tablespaces angeben.

- Wenn Einschränkungen für die Tabellen in einem Tablespace in einem anderen Tablespace enthalten sind, sollten Sie beide Tablespaces wiederherstellen
- Wenn eine Tabelle und ihre Indizes in verschiedenen Tablespaces gespeichert sind, sollten die Indizes vor der Ausführung von PITR gelöscht werden.
- PITR kann nicht verwendet werden, um den aktuellen Standard-Tablespace wiederherzustellen
- PITR kann nicht zum Wiederherstellen von Tablespaces verwendet werden, die eines der folgenden Objekte enthalten:
  - Objekte mit zugrunde liegenden Objekten (z. B. materialisierte Ansichten) oder enthaltenen Objekten (z. B. partitionierte Tabellen), es sei denn, alle zugrunde liegenden oder enthaltenen Objekte befinden sich im Wiederherstellungssatz

Wenn die Partitionen einer partitionierten Tabelle in unterschiedlichen Tablespaces gespeichert sind, sollten Sie außerdem entweder die Tabelle löschen, bevor Sie PITR ausführen, oder alle Partitionen in denselben Tablespace verschieben, bevor Sie PITR ausführen.

- Rückgängigmachen oder Zurücksetzen von Segmenten
- Oracle 8-kompatible erweiterte Warteschlangen mit mehreren Empfängern
- Objekte, die dem SYS-Benutzer gehören

Beispiele für diese Objekttypen sind PL/SQL, Java-Klassen, Callout-Programme, Ansichten, Synonyme, Benutzer, Berechtigungen, Dimensionen, Verzeichnisse und Sequenzen.

## **Quellen und Ziele für die Wiederherstellung von Oracle-Datenbanken**

Sie können eine Oracle-Datenbank aus einer Sicherungskopie auf einem Primär- oder Sekundärspeicher wiederherstellen. Sie können Datenbanken nur am selben Speicherort auf derselben Datenbankinstanz wiederherstellen. Im Real Application Cluster (RAC)-Setup können Sie Datenbanken jedoch auf anderen Knoten wiederherstellen.

### **Quellen für Wiederherstellungsvorgänge**

Sie können Datenbanken aus einer Sicherung auf dem Primär- oder Sekundärspeicher wiederherstellen. Wenn Sie in einer Konfiguration mit mehreren Spiegeln eine Wiederherstellung aus einer Sicherung auf dem sekundären Speicher durchführen möchten, können Sie den sekundären Speicherspiegel als Quelle auswählen.

### **Ziele für Wiederherstellungsvorgänge**

Sie können Datenbanken nur am selben Speicherort auf derselben Datenbankinstanz wiederherstellen.

In einem RAC-Setup können Sie RAC-Datenbanken von allen Knoten im Cluster wiederherstellen.

## **Vordefinierte Umgebungsvariablen zum Wiederherstellen bestimmter Prescript- und Postscript-Dateien**

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie beim Wiederherstellen einer Datenbank das Prescript und Postscript ausführen.

### **Unterstützte vordefinierte Umgebungsvariablen zum Wiederherstellen einer Datenbank**



- **SC\_JOB\_ID** gibt die Job-ID des Vorgangs an.

Beispiel: 257

- **SC\_ORACLE\_SID** gibt die Systemkennung der Datenbank an.

Wenn der Vorgang mehrere Datenbanken umfasst, enthält dies durch Pipes getrennte Datenbanknamen.

Beispiel: NFSB31

- **SC\_HOST** gibt den Hostnamen der Datenbank an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: scsmohost2.gdl.englabe.netapp.com

- **SC\_OS\_USER** gibt den Betriebssystembesitzer der Datenbank an.

Beispiel: Orakel

- **SC\_OS\_GROUP** gibt die Betriebssystemgruppe der Datenbank an.

Beispiel: oinstall

- **SC\_BACKUP\_NAME** gibt den Namen der Sicherung an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiele:

- Wenn die Datenbank nicht im ARCHIVELOG-Modus ausgeführt wird:  
DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-21-2021\_12.16.48.9267\_1, RG2\_scspr2417819002\_07-22-2021\_12.16.48.9267\_1

- **SC\_BACKUP\_ID** gibt die ID des Backups an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiele:

- Wenn die Datenbank nicht im ARCHIVELOG-Modus läuft: DATA@203|LOG@205
- Wenn die Datenbank im ARCHIVELOG-Modus läuft: DATA@203|LOG@205,206,207

- **SC\_RESOURCE\_GROUP\_NAME** gibt den Namen der Ressourcengruppe an.

Beispiel: RG1

- **SC\_ORACLE\_HOME** gibt den Pfad des Oracle-Home-Verzeichnisses an.

Beispiel: /ora01/app/oracle/product/18.1.0/db\_1

- **SC\_RECOVERY\_TYPE** gibt die wiederherzustellenden Dateien und den Wiederherstellungsumfang an.

Beispiel:

```
RESTORESCOPE:usingBackupControlfile=false|RECOVERYScope:allLogs=true,noLogs=false,untiltime=false,untilscn=false.
```

Informationen zu Trennzeichen finden Sie unter ["Unterstützte Trennzeichen"](#) .

## Voraussetzungen für die Wiederherstellung einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank wiederherstellen, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie sollten Ihre Wiederherstellungs- und Recovery-Strategie definiert haben.
- Der SnapCenter Administrator sollte Ihnen die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben, wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren.
- Wenn Archivprotokolle im Rahmen der Sicherung bereinigt werden, sollten Sie die erforderlichen Archivprotokollsicherungen manuell bereitgestellt haben.
- Wenn Sie Oracle-Datenbanken wiederherstellen möchten, die sich auf einer Virtual Machine Disk (VMDK) befinden, sollten Sie sicherstellen, dass die Gastmaschine über die erforderliche Anzahl freier Steckplätze für die Zuweisung der geklonten VMDKs verfügt.
- Sie sollten sicherstellen, dass alle zur Datenbank gehörenden Datenvolumes und Archivprotokollvolumes geschützt sind, wenn für diese Datenbank der sekundäre Schutz aktiviert ist.
- Sie sollten sicherstellen, dass sich die RAC One Node-Datenbank im Status „nomount“ befindet, um eine Steuerdatei oder eine vollständige Datenbankwiederherstellung durchzuführen.
- Wenn Sie über eine ASM-Datenbankinstanz in einer NFS-Umgebung verfügen, sollten Sie den ASM-Festplattenpfad `/var/opt/snapcenter/scu/clones/*/*` zum vorhandenen Pfad hinzufügen, der im Parameter `asm_diskstring` definiert ist, um die ASM-Protokollsicherungen als Teil des Wiederherstellungsvorgangs erfolgreich bereitzustellen.
- Im Parameter `asm_diskstring` sollten Sie `AFD:*` konfigurieren, wenn Sie ASMFD verwenden, oder `ORCL:*`, wenn Sie ASMLIB verwenden.



Informationen zum Bearbeiten des Parameters `asm_diskstring` finden Sie unter ["So fügen Sie Datenträgerpfade zu asm\\_diskstring hinzu"](#)

- Sie sollten den statischen Listener in der Datei **listener.ora** konfigurieren, die unter `$ORACLE_HOME/network/admin` für Nicht-ASM-Datenbanken und unter `$GRID_HOME/network/admin` für ASM-Datenbanken verfügbar ist, wenn Sie die Betriebssystemauthentifizierung deaktiviert und die Oracle-Datenbankauthentifizierung für eine Oracle-Datenbank aktiviert haben und die Datendateien und Steuerdateien dieser Datenbank wiederherstellen möchten.
- Sie sollten den Wert des `SCORestoreTimeout`-Parameters erhöhen, indem Sie den Befehl `Set-SmConfigSettings` ausführen, wenn die Datenbankgröße in Terabyte (TB) angegeben ist.
- Sie sollten sicherstellen, dass alle für vCenter erforderlichen Lizenzen installiert und auf dem neuesten Stand sind.

Wenn die Lizenzen nicht installiert oder nicht auf dem neuesten Stand sind, wird eine Warnmeldung angezeigt. Wenn Sie die Warnung ignorieren und fortfahren, schlägt die Wiederherstellung von RDM fehl.

- Sie sollten sicherstellen, dass die LUN nicht mithilfe einer iGroup, die aus gemischten Protokollen iSCSI und FC besteht, auf den AIX-Host abgebildet wird. Weitere Informationen finden Sie unter ["Der Vorgang"](#)

schlägt mit dem Fehler „Gerät für LUN konnte nicht erkannt werden“ fehl.“ .

## Wiederherstellen und Wiederherstellen der Oracle-Datenbank

Im Falle eines Datenverlusts können Sie mit SnapCenter Daten aus einem oder mehreren Backups auf Ihrem aktiven Dateisystem wiederherstellen und anschließend die Datenbank wiederherstellen.

### Bevor Sie beginnen

Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

### Über diese Aufgabe

- Die Wiederherstellung erfolgt mithilfe der Archivprotokolle, die am konfigurierten Archivprotokollspeicherort verfügbar sind. Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird, speichert die Oracle-Datenbank die gefüllten Gruppen von Redo-Log-Dateien an einem oder mehreren Offline-Zielen, die zusammen als archiviertes Redo-Log bezeichnet werden. SnapCenter ermittelt und mountet die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN, dem ausgewählten Datum und der Uhrzeit oder der Option „Alle Protokolle“. Wenn die für die Wiederherstellung erforderlichen Archivprotokolle am konfigurierten Speicherort nicht verfügbar sind, sollten Sie den Snapshot mit den Protokollen mounten und den Pfad als externe Archivprotokolle angeben.

Wenn Sie die ASM-Datenbank von ASMLIB nach ASMFD migrieren, können die mit ASMLIB erstellten Sicherungen nicht zum Wiederherstellen der Datenbank verwendet werden. Sie sollten in der ASMFD-Konfiguration Sicherungen erstellen und diese Sicherungen zur Wiederherstellung verwenden. Wenn die ASM-Datenbank von ASMFD nach ASMLIB migriert wird, sollten Sie zur Wiederherstellung Sicherungen in der ASMLIB-Konfiguration erstellen.

Wenn Sie eine Datenbank wiederherstellen, wird auf dem Oracle-Datenbankhost im Verzeichnis `/var/opt/snapcenter/sco/lock` eine Betriebssperrdatei (`.sm_lock_dbsid`) erstellt, um zu vermeiden, dass mehrere Vorgänge auf der Datenbank ausgeführt werden. Nach der Wiederherstellung der Datenbank wird die Betriebssperrdatei automatisch entfernt.



Die Wiederherstellung der SPFILE- und Kennwortdatei wird nicht unterstützt.

- 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.

### 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank entweder aus der Datenbankdetailansicht oder der Ressourcengruppendetailansicht aus.

Die Seite „Datenbanktopologie“ 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. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
  - a. Wenn Sie eine Sicherung einer Datenbank in einer Real Application Clusters (RAC)-Umgebung ausgewählt haben, wählen Sie den RAC-Knoten aus.
  - b. Wenn Sie gespiegelte oder Tresordaten auswählen:
    - Wenn es keine Protokollsicherung im Spiegel oder Tresor gibt, wird nichts ausgewählt und die Locatoren sind leer.
    - Wenn Protokollsicherungen im Spiegel oder Tresor vorhanden sind, wird die neueste Protokollsicherung ausgewählt und der entsprechende Locator angezeigt.



Wenn die ausgewählte Protokollsicherung sowohl am Spiegel- als auch am Tresorspeicherort vorhanden ist, werden beide Locatoren angezeigt.

- c. Führen Sie die folgenden Aktionen aus:

| Wenn Sie wiederherstellen möchten... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alle Datendateien der Datenbank      | <p>Wählen Sie <b>Alle Datendateien</b>.</p> <p>Es werden nur die Datendateien der Datenbank wiederhergestellt. Die Steuerdateien, Archivprotokolle oder Redo-Log-Dateien werden nicht wiederhergestellt.</p>                                                                                                                                                                                                                                                                                                                                   |
| Tabellenbereiche                     | <p>Wählen Sie <b>Tablespaces</b> aus.</p> <p>Sie können die Tablespaces angeben, die Sie wiederherstellen möchten.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Steuerdateien                        | <p>Wählen Sie <b>Steuerdateien</b>.</p> <div>  <p>Stellen Sie beim Wiederherstellen von Steuerdateien sicher, dass die Verzeichnisstruktur entweder vorhanden ist oder mit den richtigen Benutzer- und Gruppeneigentümern (sofern vorhanden) erstellt wird, damit die Dateien beim Wiederherstellungsprozess an den Zielspeicherort kopiert werden können. Wenn das Verzeichnis nicht vorhanden ist, schlägt der Wiederherstellungsauftrag fehl.</p> </div> |

| Wenn Sie wiederherstellen möchten...      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Redo-Log-Dateien                          | <p>Wählen Sie <b>Protokolldateien wiederholen</b>.</p> <p>Diese Option ist nur für Data Guard-Standby- oder Active Data Guard-Standby-Datenbanken verfügbar.</p> <div>  <p>Für Datenbanken, die nicht zu Data Guard gehören, werden keine Redo-Log-Dateien gesichert. Bei Datenbanken, die nicht von Data Guard stammen, wird die Wiederherstellung mithilfe von Archivprotokollen durchgeführt.</p> </div> |
| Pluggable-Datenbanken (PDBs)              | Wählen Sie <b>Pluggable-Datenbanken</b> aus und geben Sie dann die PDBs an, die Sie wiederherstellen möchten.                                                                                                                                                                                                                                                                                                                                                                                |
| Pluggable Database (PDB)-Tabellenbereiche | <p>Wählen Sie <b>Pluggable Database (PDB)-Tablespaces</b> aus und geben Sie dann die PDB und die Tablespaces dieser PDB an, die Sie wiederherstellen möchten.</p> <p>Diese Option ist nur verfügbar, wenn Sie eine PDB zur Wiederherstellung ausgewählt haben.</p>                                                                                                                                                                                                                           |

- d. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.

Die verschiedenen Zustände einer Datenbank sind (von oben nach unten) geöffnet, gemountet, gestartet und heruntergefahren. Sie müssen dieses Kontrollkästchen aktivieren, wenn sich die Datenbank in einem höheren Status befindet, der Status jedoch in einen niedrigeren Status geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen. Wenn sich die Datenbank in einem niedrigeren Status befindet, der Status jedoch in einen höheren Status geändert werden muss, um den Wiederherstellungsvorgang durchzuführen, wird der Datenbankstatus automatisch geändert, auch wenn Sie das Kontrollkästchen nicht aktivieren.

Wenn sich eine Datenbank im geöffneten Zustand befindet und für die Wiederherstellung der Zustand „gemountet“ erforderlich ist, wird der Datenbankstatus nur geändert, wenn Sie dieses Kontrollkästchen aktivieren.

- a. Wählen Sie **In-Place-Wiederherstellung erzwingen**, wenn Sie eine In-Place-Wiederherstellung in Szenarien durchführen möchten, in denen nach der Sicherung neue Datendateien hinzugefügt werden oder wenn LUNs zu einer LVM-Datenträgergruppe hinzugefügt, gelöscht oder neu erstellt werden.

7. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aktionen aus:

| Wenn du...                                                                 | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Möchten Sie die letzte Transaktion wiederherstellen                        | Wählen Sie <b>Alle Protokolle</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Möchten Sie auf eine bestimmte System Change Number (SCN) wiederherstellen | Wählen Sie <b>Bis SCN (System Change Number)</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Möchten Sie zu einem bestimmten Datum und Zeitpunkt wiederherstellen       | Wählen Sie <b>Datum und Uhrzeit</b> .<br><br>Sie müssen Datum und Uhrzeit der Zeitzone des Datenbankhosts angeben.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Will nicht erholen                                                         | Wählen Sie <b>Keine Wiederherstellung</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Möchten Sie externe Archivprotokollspeicherorte angeben                    | <p>Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird, ermittelt und mountet SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN, dem ausgewählten Datum und der Uhrzeit oder der Option „Alle Protokolle“.</p> <p>Wenn Sie dennoch den Speicherort der externen Archivprotokolldateien angeben möchten, wählen Sie <b>Speicherorte für externe Archivprotokolle angeben</b>.</p> <p>Wenn Archivprotokolle im Rahmen der Sicherung bereinigt werden und Sie die erforderlichen Archivprotokollsicherungen manuell bereitgestellt haben, müssen Sie den bereitgestellten Sicherungspfad als externen Archivprotokollspeicherort für die Wiederherstellung angeben.</p> <div>  <p>Sie sollten den Pfad und den Inhalt des Mount-Pfads überprüfen, bevor Sie ihn als externen Protokollspeicherort auflisten.</p> </div> <ul style="list-style-type: none"> <li>• <a href="#">"Oracle-Datenschutz mit ONTAP"</a></li> <li>• <a href="#">"Der Vorgang schlägt mit dem Fehler ORA-00308 fehl"</a></li> </ul> |

Sie können keine Wiederherstellung mit der Wiederherstellung aus sekundären Sicherungen durchführen, wenn die Archivprotokollvolumes nicht geschützt sind, die Datenvolumes jedoch geschützt sind. Sie können nur wiederherstellen, indem Sie **Keine Wiederherstellung** auswählen.

Wenn Sie eine RAC-Datenbank mit ausgewählter Option „Datenbank öffnen“ wiederherstellen, wird nur die RAC-Instanz, bei der der Wiederherstellungsvorgang initiiert wurde, wieder in den geöffneten Zustand versetzt.



Die Wiederherstellung wird für Data Guard-Standby- und Active Data Guard-Standby-Datenbanken nicht unterstützt.

8. Geben Sie auf der Seite „PreOps“ den Pfad und die Argumente des Prescripts ein, das Sie vor dem Wiederherstellungsvorgang ausführen möchten.

Sie müssen die Prescripts entweder im Pfad `/var/opt/snapcenter/spl/scripts` oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad `/var/opt/snapcenter/spl/scripts` ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

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

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen. "[Mehr erfahren](#)"

9. Führen Sie auf der Seite „PostOps“ die folgenden Schritte aus:

- a. Geben Sie den Pfad und die Argumente des Postscripts ein, das Sie nach dem Wiederherstellungsvorgang ausführen möchten.

Sie müssen die Postscripts entweder in `/var/opt/snapcenter/spl/scripts` oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad `/var/opt/snapcenter/spl/scripts` ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.



Wenn der Wiederherstellungsvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungsaktivitäten direkt ausgelöst.

- b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

Wenn Sie nach der Wiederherstellung einer Containerdatenbank (CDB) mit oder ohne Steuerdateien oder nach der Wiederherstellung nur der CDB-Steuerdateien angeben, dass die Datenbank nach der Wiederherstellung geöffnet werden soll, wird nur die CDB geöffnet und nicht die Pluggable Databases (PDB) in dieser CDB.

In einem RAC-Setup wird nach der Wiederherstellung nur die RAC-Instanz geöffnet, die für die Wiederherstellung verwendet wird.



Nach der Wiederherstellung eines Benutzertabellenbereichs mit Steuerdateien, eines Systemtabellenbereichs mit oder ohne Steuerdateien oder einer PDB mit oder ohne Steuerdateien wird nur der Status der PDB im Zusammenhang mit dem Wiederherstellungsvorgang in den ursprünglichen Status geändert. Der Status der anderen PDBs, die nicht für die Wiederherstellung verwendet wurden, wird nicht in den ursprünglichen Status zurückgesetzt, da der Status dieser PDBs nicht gespeichert wurde. Sie müssen den Status der PDBs, die nicht für die Wiederherstellung verwendet wurden, manuell ändern.

10. 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-SmSmtServer“ angegeben haben.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

#### Für weitere Informationen

- ["Die Oracle RAC One Node-Datenbank wird für die Durchführung von SnapCenter -Vorgängen übersprungen"](#)
- ["Die Wiederherstellung von einem sekundären SnapMirror oder SnapVault Speicherort ist fehlgeschlagen."](#)
- ["Fehler beim Wiederherstellen aus einer Sicherung einer verwaisten Inkarnation"](#)
- ["Anpassbare Parameter für Sicherungs-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"](#)

## Wiederherstellen und Wiederherstellen von Tablespaces mithilfe der Point-in-Time-Wiederherstellung

Sie können eine Teilmenge der Tablespaces wiederherstellen, die beschädigt oder gelöscht wurde, ohne dass dies Auswirkungen auf die anderen Tablespaces in der Datenbank hat. SnapCenter verwendet RMAN, um eine Point-in-Time-Wiederherstellung (PITR) der Tablespaces durchzuführen.

#### Bevor Sie beginnen

- Die für die PITR-Durchführung von Tablespaces erforderlichen Sicherungen sollten katalogisiert und gemountet werden.
- Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

#### Über diese Aufgabe

Während des PITR-Vorgangs erstellt RMAN eine Hilfsinstanz am angegebenen Hilfsziel. Das zusätzliche Ziel könnte ein Einhängpunkt oder eine ASM-Datenträgergruppe sein. Wenn am bereitgestellten Speicherort ausreichend Speicherplatz vorhanden ist, können Sie anstelle eines dedizierten Bereitstellungspunkts einen der bereitgestellten Speicherorte wiederverwenden.

Sie sollten Datum und Uhrzeit oder SCN angeben und der Tablespace wird in der Quelldatenbank wiederhergestellt.

Sie können mehrere Tablespaces auswählen und wiederherstellen, die sich in ASM-, NFS- und SAN-Umgebungen befinden. Wenn sich beispielsweise die Tablespaces TS2 und TS3 auf NFS und TS4 auf SAN befinden, können Sie einen einzelnen PITR-Vorgang ausführen, um alle Tablespaces wiederherzustellen.



In einem RAC-Setup können Sie PITR von Tablespaces von jedem Knoten des RAC aus durchführen.

#### 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (mehrere Mandanten)“ entweder aus der Datenbankdetailansicht oder der Ressourcengruppendetailansicht aus.

Die Seite „Datenbanktopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder vom primären oder vom sekundären (gespiegelten oder replizierten) Speichersystem aus.

Wenn das Backup nicht katalogisiert ist, sollten Sie das Backup auswählen und auf **Katalog** klicken.

5. Wählen Sie das katalogisierte Backup aus und klicken Sie dann auf \*  \*.

6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:

- a. Wenn Sie eine Sicherung einer Datenbank in einer Real Application Clusters (RAC)-Umgebung ausgewählt haben, wählen Sie den RAC-Knoten aus.
- b. Wählen Sie **Tablespaces** aus und geben Sie dann die Tablespaces an, die Sie wiederherstellen möchten.



Sie können PITR nicht auf SYSAUX-, SYSTEM- und UNDO-Tablespaces ausführen.

- c. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.
7. Führen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Aktionen aus:
    - Wenn Sie zu einer bestimmten System Change Number (SCN) wiederherstellen möchten, wählen Sie **Bis SCN** und geben Sie die SCN und das Zusatzziel an.
    - Wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten, wählen Sie **Datum und Uhrzeit** und geben Sie Datum und Uhrzeit sowie das zusätzliche Ziel an.

SnapCenter ermittelt und mountet und katalogisiert anschließend die optimale Anzahl an Daten- und Protokollsicherungen, die zum Durchführen von PITR basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit erforderlich sind.

8. Geben Sie auf der Seite „PreOps“ den Pfad und die Argumente des Prescripts ein, das Sie vor dem Wiederherstellungsvorgang ausführen möchten.

Sie sollten die Prescripts entweder im Pfad /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig ist der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

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

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen. ["Mehr erfahren"](#)

9. Führen Sie auf der Seite „PostOps“ die folgenden Schritte aus:

- a. Geben Sie den Pfad und die Argumente des Postscripts ein, das Sie nach dem Wiederherstellungsvorgang ausführen möchten.



Wenn der Wiederherstellungsvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungsaktivitäten direkt ausgelöst.

- b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

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

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

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

## Wiederherstellen und Wiederherstellen einer steckbaren Datenbank mithilfe der Point-in-Time-Wiederherstellung

Sie können eine Pluggable Database (PDB), die beschädigt oder gelöscht wurde, wiederherstellen, ohne dass dies Auswirkungen auf die anderen PDBs in der Containerdatenbank (CDB) hat. SnapCenter verwendet RMAN, um eine Point-in-Time-Wiederherstellung (PITR) der PDB durchzuführen.

### Bevor Sie beginnen

- Die Sicherungen, die zum Ausführen von PITR eines PDB erforderlich sind, sollten katalogisiert und bereitgestellt werden.



In einem RAC-Setup sollten Sie die PDB auf allen Knoten des RAC-Setups manuell schließen (indem Sie den Status in „MOUNTED“ ändern).

- Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

### Über diese Aufgabe

Während des PITR-Vorgangs erstellt RMAN eine Hilfsinstanz am angegebenen Hilfsziel. Das zusätzliche Ziel könnte ein Einhängpunkt oder eine ASM-Datenträgergruppe sein. Wenn am bereitgestellten Speicherort ausreichend Speicherplatz vorhanden ist, können Sie anstelle eines dedizierten Bereitstellungspunkts einen der bereitgestellten Speicherorte wiederverwenden.

Sie sollten Datum und Uhrzeit oder SCN angeben, um PITR des PDB durchzuführen. RMAN kann READ WRITE, READ ONLY oder gelöschte PDBs einschließlich Datendateien wiederherstellen.

Sie können nur Folgendes wiederherstellen und wiederherstellen:

- jeweils ein PDB
- ein Tablespace in einer PDB
- mehrere Tablespaces derselben PDB



In einem RAC-Setup können Sie PITR von Tablespaces von jedem Knoten des RAC aus durchführen.

## 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (mehrere Mandanten)“ entweder aus der Datenbankdetailansicht oder der Ressourcengruppendetailansicht aus.

Die Seite „Datenbanktopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder vom primären oder vom sekundären (gespiegelten oder replizierten) Speichersystem aus.

Wenn das Backup nicht katalogisiert ist, sollten Sie das Backup auswählen und auf **Katalog** klicken.

5. Wählen Sie das katalogisierte Backup aus und klicken Sie dann auf \*  \*.

6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:

- a. Wenn Sie eine Sicherung einer Datenbank in einer Real Application Clusters (RAC)-Umgebung ausgewählt haben, wählen Sie den RAC-Knoten aus.
- b. Führen Sie eine der folgenden Aktionen aus, je nachdem, ob Sie die PDB oder Tablespaces in einer PDB wiederherstellen möchten:

| Wenn Sie wollen...         | Schritte...                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wiederherstellen einer PDB | <ol style="list-style-type: none"><li>i. Wählen Sie <b>Pluggable-Datenbanken (PDBs)</b> aus.</li><li>ii. Geben Sie die PDB an, die Sie wiederherstellen möchten.</li></ol> <div><p>Sie können PITR nicht auf der PDB\$SEED-Datenbank ausführen.</p></div> |

Wiederherstellen von Tablespaces in einer PDB

i. Wählen Sie **Pluggable Database (PDB)-Tablespaces** aus.

ii. Geben Sie den PDB an.

iii. Geben Sie entweder einen einzelnen oder mehrere Tablespaces an, die Sie wiederherstellen möchten.



Sie können PITR nicht auf SYSAUX-, SYSTEM- und UNDO-Tablespaces ausführen.

c. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.

7. Führen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Aktionen aus:

- Wenn Sie zu einer bestimmten System Change Number (SCN) wiederherstellen möchten, wählen Sie **Bis SCN** und geben Sie die SCN und das Zusatzziel an.
- Wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten, wählen Sie **Datum und Uhrzeit** und geben Sie Datum und Uhrzeit sowie das zusätzliche Ziel an.

SnapCenter ermittelt und mountet und katalogisiert anschließend die optimale Anzahl an Daten- und Protokollsicherungen, die zum Durchführen von PITR basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit erforderlich sind.

8. Geben Sie auf der Seite „PreOps“ den Pfad und die Argumente des Prescripts ein, das Sie vor dem Wiederherstellungsvorgang ausführen möchten.

Sie sollten die Prescripts entweder im Pfad /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig ist der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie innerhalb dieses Pfads Ordner zum Speichern der Skripte erstellt haben, müssen Sie diese Ordner im Pfad angeben.

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

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen. ["Mehr erfahren"](#)

9. Führen Sie auf der Seite „PostOps“ die folgenden Schritte aus:

- a. Geben Sie den Pfad und die Argumente des Postscripts ein, das Sie nach dem Wiederherstellungsvorgang ausführen möchten.



Wenn der Wiederherstellungsvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungsaktivitäten direkt ausgelöst.

- b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

In einem RAC-Setup wird die PDB nur auf dem Knoten geöffnet, auf dem die Datenbank

wiederhergestellt wurde. Sie sollten die wiederhergestellte PDB manuell auf allen anderen Knoten des RAC-Setups öffnen.

10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

## Wiederherstellen und Wiederherstellen von Oracle-Datenbanken mit UNIX-Befehlen

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungs- und Recovery-Vorgänge sowie die Überwachung der Vorgänge.

### 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. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer: *Open-SmConnection*
2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten: *Get-SmBackup*
3. Rufen Sie die detaillierten Informationen zum angegebenen Backup ab: *Get-SmBackupDetails*

Dieser Befehl ruft die detaillierten Informationen zur Sicherung einer angegebenen Ressource mit einer bestimmten Sicherungs-ID ab. Die Informationen umfassen Datenbankname, Version, Home, Start- und End-SCN, Tablespace, Pluggable-Datenbanken und deren Tablespace.

4. Daten aus dem Backup wiederherstellen: *Restore-SmBackup*

## Überwachen von Wiederherstellungsvorgängen für Oracle-Datenbanken

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.

## Abbrechen von Oracle-Datenbankwiederherstellungsvorgängen

Sie können in der Warteschlange befindliche Wiederherstellungsaufträge abbrechen.

Sie sollten als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

### Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Wiederherstellungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li><li>2. Wählen Sie den Auftrag aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                                     |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>2. Wählen Sie den Vorgang aus.</li><li>3. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li></ol> |

## Oracle-Datenbank klonen

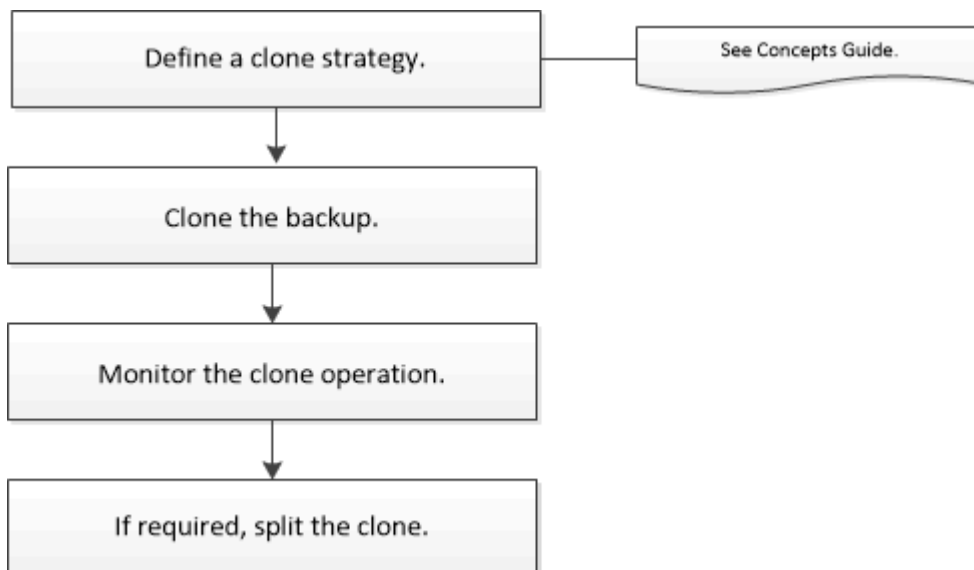
### Klon-Workflow

Der Klon-Workflow umfasst die Planung, Durchführung und Überwachung des Klonvorgangs.

Sie können Datenbanken aus den folgenden Gründen klonen:

- Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mithilfe der aktuellen Datenbankstruktur und des aktuellen Datenbankinhalts implementiert werden müssen.
- Zum Befüllen von Data Warehouses mithilfe von Tools zur Datenextraktion und -bearbeitung.
- Um Daten wiederherzustellen, die versehentlich gelöscht oder geändert wurden.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



## Definieren Sie eine Klonstrategie für Oracle-Datenbanken

Durch die Definition einer Strategie vor dem Klonen Ihrer Datenbank wird sichergestellt, dass der Klonvorgang erfolgreich ist.

### Für das Klonen unterstützte Sicherungstypen

SnapCenter unterstützt das Klonen verschiedener Arten von Backups von Oracle-Datenbanken.

- Online-Datensicherung
- Online-Vollsicherung
- Offline-Mount-Backup
- Offline-Shutdown-Backup
- Sicherungen von Data Guard-Standby-Datenbanken und Active Data Guard-Standby-Datenbanken
- Online-Datensicherungen, Online-Vollsicherungen, Offline-Mount-Sicherungen und Offline-Shutdown-Sicherungen in einer Real Application Clusters (RAC)-Konfiguration
- Online-Datensicherungen, Online-Vollsicherungen, Offline-Mount-Sicherungen und Offline-Shutdown-Sicherungen in einer Automatic Storage Management (ASM)-Konfiguration



SAN-Konfigurationen werden nicht unterstützt, wenn die Option „user\_friendly\_names“ in der Multipath-Konfigurationsdatei auf „yes“ gesetzt ist.



Das Klonen von Archivprotokollsicherungen wird nicht unterstützt.

### Für Oracle-Datenbanken unterstützte Klontypen

In einer Oracle-Datenbankumgebung unterstützt SnapCenter das Klonen einer Datenbanksicherung. Sie können das Backup von primären und sekundären Speichersystemen klonen.

Der SnapCenter Server verwendet die NetApp FlexClone -Technologie zum Klonen von Backups.

Sie können einen Klon aktualisieren, indem Sie den Befehl „Refresh-SmClone“ ausführen. Dieser Befehl erstellt eine Sicherungskopie der Datenbank, löscht den vorhandenen Klon und erstellt einen Klon mit demselben Namen.



Der Klonaktualisierungsvorgang kann nur mithilfe der UNIX-Befehle durchgeführt werden.

### Klon-Namenskonventionen für Oracle-Datenbanken

Ab SnapCenter 3.0 unterscheidet sich die für Klone von Dateisystemen verwendete Namenskonvention von der für Klone von ASM-Datenträgergruppen.

- Die Namenskonvention für SAN- oder NFS-Dateisysteme lautet „FileSystemNameofsourcedatabase\_CLONESID“.
- Die Namenskonvention für ASM-Datenträgergruppen lautet SC\_HASHCODEofDISKGROUP\_CLONESID.

HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Datenträgergruppe eindeutig ist.



## Einschränkungen beim Klonen von Oracle-Datenbanken

Sie sollten sich der Einschränkungen von Klonvorgängen bewusst sein, bevor Sie die Datenbanken klonen.

- Wenn Sie eine beliebige Version von Oracle zwischen 11.2.0.4 und 12.1.0.1 verwenden, bleibt der Klonvorgang hängen, wenn Sie den Befehl *renamedg* ausführen. Sie können den Oracle-Patch 19544733 anwenden, um dieses Problem zu beheben.
- Das Klonen von Datenbanken von einer LUN, die direkt an einen Host angeschlossen ist (z. B. mithilfe des Microsoft iSCSI-Initiators auf einem Windows-Host), auf eine VMDK oder eine RDM-LUN auf demselben oder einem anderen Windows-Host oder umgekehrt wird nicht unterstützt.
- Das Stammverzeichnis des Volume-Mount-Punkts darf kein freigegebenes Verzeichnis sein.
- Wenn Sie eine LUN, die einen Klon enthält, auf ein neues Volume verschieben, kann der Klon nicht gelöscht werden.

## Vordefinierte Umgebungsvariablen für klonspezifisches Prescript und Postscript

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie beim Klonen einer Datenbank das Prescript und Postscript ausführen.

### Unterstützte vordefinierte Umgebungsvariablen zum Klonen einer Datenbank

- **SC\_ORIGINAL\_SID** gibt die SID der Quelldatenbank an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: NFSB32

- **SC\_ORIGINAL\_HOST** gibt den Namen des Quellhosts an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: asmrac1.gdl.englab.netapp.com

- **SC\_ORACLE\_HOME** gibt den Pfad des Oracle-Home-Verzeichnisses der Zieldatenbank an.

Beispiel: /ora01/app/oracle/product/18.1.0/db\_1

- **SC\_BACKUP\_NAME** gibt den Namen der Sicherung an.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiele:

- Wenn die Datenbank nicht im ARCHIVELOG-Modus ausgeführt wird:  
DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird: DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG:RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1,RG2\_scspr2417819002\_07-21-2021\_12.16.48.9267\_1,RG2\_scspr2417819002\_07-22-2021\_12.16.48.9267\_1

- **SC\_AV\_NAME** gibt die Namen der Anwendungsvolumes an.

Beispiel: AV1|AV2

- **SC\_ORIGINAL\_OS\_USER** gibt den Betriebssystembesitzer der Quelldatenbank an.

Beispiel: Orakel

- **SC\_ORIGINAL\_OS\_GROUP** gibt die Betriebssystemgruppe der Quelldatenbank an.

Beispiel: oinstall

- **SC\_TARGET\_SID** gibt die SID der geklonten Datenbank an.

Für den PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: clonedb

- **SC\_TARGET\_HOST** gibt den Namen des Hosts an, auf dem die Datenbank geklont wird.

Dieser Parameter wird für Anwendungsvolumes ausgefüllt.

Beispiel: asmrac1.gdl.englab.netapp.com

- **SC\_TARGET\_OS\_USER** gibt den Betriebssystembesitzer der geklonten Datenbank an.

Für den PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

Beispiel: Orakel

- **SC\_TARGET\_OS\_GROUP** gibt die Betriebssystemgruppe der geklonten Datenbank an.

Für den PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

Beispiel: oinstall

- **SC\_TARGET\_DB\_PORT** gibt den Datenbankport der geklonten Datenbank an.

Für den PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

Beispiel: 1521

Informationen zu Trennzeichen finden Sie unter "[Unterstützte Trennzeichen](#)".

## Voraussetzungen für das Klonen einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank klonen, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie sollten mit SnapCenter eine Sicherungskopie der Datenbank erstellt haben.

Damit der Klonvorgang erfolgreich ist, sollten Sie erfolgreich Online-Daten- und Protokollsicherungen oder Offline-Sicherungen (Mounten oder Herunterfahren) erstellt haben.

- Wenn Sie die Pfade der Steuerdatei oder der Redo-Log-Datei anpassen möchten, sollten Sie das erforderliche Dateisystem oder die Automatic Storage Management (ASM)-Datenträgergruppe vorab bereitgestellt haben.

Standardmäßig werden Redo-Log- und Steuerdateien der geklonten Datenbank auf der ASM-Datenträgergruppe oder dem von SnapCenter bereitgestellten Dateisystem für die Datendateien der Klondatenbank erstellt.

- Wenn Sie ASM über NFS verwenden, sollten Sie `/var/opt/snapcenter/scu/clones/*/*` zum vorhandenen Pfad hinzufügen, der im Parameter `asm_diskstring` definiert ist.
- Im Parameter `asm_diskstring` sollten Sie `AFD:*` konfigurieren, wenn Sie ASMFD verwenden, oder `ORCL:*`, wenn Sie ASMLIB verwenden.

Informationen zum Bearbeiten des Parameters `asm_diskstring` finden Sie unter ["So fügen Sie Datenträgerpfade zu asm\\_diskstring hinzu"](#) .

- Wenn Sie den Klon auf einem alternativen Host erstellen, sollte der alternative Host die folgenden Anforderungen erfüllen:
  - Das SnapCenter Plug-in für Oracle-Datenbanken sollte auf dem alternativen Host installiert werden.
  - Der Klonhost sollte in der Lage sein, LUNs vom primären oder sekundären Speicher zu erkennen.
    - Wenn Sie vom primären Speicher oder sekundären Speicher (Vault oder Mirror) auf einen alternativen Host klonen, stellen Sie sicher, dass entweder eine iSCSI-Sitzung zwischen dem sekundären Speicher und dem alternativen Host hergestellt oder für FC ordnungsgemäß in Zonen eingeteilt wird.
    - Wenn Sie vom Vault- oder Mirror-Speicher auf denselben Host klonen, stellen Sie sicher, dass entweder eine iSCSI-Sitzung zwischen dem Vault- oder Mirror-Speicher und dem Host hergestellt oder für FC ordnungsgemäß in Zonen eingeteilt ist.
    - Wenn Sie in einer virtualisierten Umgebung klonen, stellen Sie sicher, dass entweder eine iSCSI-Sitzung zwischen dem primären oder sekundären Speicher und dem ESX-Server, auf dem sich der alternative Host befindet, hergestellt oder eine ordnungsgemäße Zoneneinteilung für FC erfolgt.

Weitere Informationen finden Sie unter ["Dokumentation zu Host-Dienstprogrammen"](#) .

- Wenn die Quelldatenbank eine ASM-Datenbank ist:
  - Die ASM-Instanz sollte auf dem Host, auf dem der Klon ausgeführt wird, aktiv sein.
  - Die ASM-Datenträgergruppe sollte vor dem Klonvorgang bereitgestellt werden, wenn Sie Archivprotokolldateien der geklonten Datenbank in einer dedizierten ASM-Datenträgergruppe platzieren möchten.
  - Der Name der Datenträgergruppe kann konfiguriert werden. Stellen Sie jedoch sicher, dass der Name nicht von einer anderen ASM-Datenträgergruppe auf dem Host verwendet wird, auf dem der Klon ausgeführt wird.

Datendateien, die sich auf der ASM-Datenträgergruppe befinden, werden als Teil des SnapCenter -Klon-Workflows bereitgestellt.

- Für NVMe sollte NVMe util installiert sein
- Der Schutztyp für die Daten-LUN und die Protokoll-LUN, z. B. Spiegel, Tresor oder Spiegel-Tresor, sollte identisch sein, um beim Klonen auf einen alternativen Host mithilfe von Protokollsicherungen sekundäre Locatoren zu erkennen.
- Sie sollten den Wert von `exclude_seed_cdb_view` in der Parameterdatei der Quelldatenbank auf `FALSE` setzen, um Seed-PDB-bezogene Informationen zum Klonen einer Sicherung der `12_c_`-Datenbank abzurufen.

Das Seed-PDB ist eine vom System bereitgestellte Vorlage, die die CDB zum Erstellen von PDBs

verwenden kann. Der Seed-PDB heißt PDB\$SEED. Informationen zu PDB\$SEED finden Sie in der Oracle-Dokument-ID 1940806.1.



Sie sollten den Wert festlegen, bevor Sie die 12\_c\_-Datenbank sichern.

- SnapCenter unterstützt die Sicherung von Dateisystemen, die vom Autofs-Subsystem verwaltet werden. Wenn Sie die Datenbank klonen, stellen Sie sicher, dass sich die Datenmountpunkte nicht unter dem Stammverzeichnis des Autofs-Mountpunkts befinden, da der Root-Benutzer des Plug-In-Hosts nicht über die Berechtigung verfügt, Verzeichnisse unter dem Stammverzeichnis des Autofs-Mountpunkts zu erstellen.

Wenn sich die Steuer- und Redo-Log-Dateien unter dem Datenmount-Punkt befinden, sollten Sie den Pfad der Steuerdatei und dann den Pfad der Redo-Log-Datei entsprechend ändern.



Sie können die neuen geklonten Einhängepunkte manuell beim Autofs-Subsystem registrieren. Die neuen geklonten Einhängepunkte werden nicht automatisch registriert.

- Wenn Sie über ein TDE (Auto-Login) verfügen und die Datenbank auf demselben oder einem anderen Host klonen möchten, sollten Sie die Wallet (Schlüsseldateien) unter `/etc/ORACLE/WALLET/$ORACLE_SID` von der Quelldatenbank in die geklonte Datenbank kopieren.
- Sie sollten den Wert von `use_lvmetad = 0` in `/etc/lvm/lvm.conf` festlegen und den Dienst `lvm2-lvmetad` stoppen, um das Klonen in Storage Area Network (SAN)-Umgebungen unter Oracle Linux 7 oder höher oder Red Hat Enterprise Linux (RHEL) 7 oder höher erfolgreich durchzuführen.
- Sie sollten den Oracle-Patch 13366202 installieren, wenn Sie die Oracle-Datenbank 11.2.0.3 oder höher verwenden und die Datenbank-ID für die Hilfsinstanz mithilfe eines NID-Skripts geändert wird.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Wenn bei NVMe ein Zielport von der Verbindung ausgeschlossen werden muss, sollten Sie den Zielknotenamen und den Portnamen in der Datei `/var/opt/snapcenter/scu/etc/nvme.conf` hinzufügen.

Wenn die Datei nicht vorhanden ist, sollten Sie die Datei wie im folgenden Beispiel gezeigt erstellen:

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- Sie sollten sicherstellen, dass die LUN nicht mithilfe einer iGroup, die aus gemischten Protokollen iSCSI und FC besteht, auf den AIX-Host abgebildet wird. Weitere Informationen finden Sie unter ["Der Vorgang schlägt mit dem Fehler „Gerät für LUN konnte nicht erkannt werden“ fehl."](#)

## Klonen einer Oracle-Datenbanksicherung

Sie können SnapCenter verwenden, um eine Oracle-Datenbank mithilfe der Sicherung der Datenbank zu klonen.

### Bevor Sie beginnen

Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für

die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

## Über diese Aufgabe

- Der Klonvorgang erstellt eine Kopie der Datenbankdateien und erstellt neue Online-Redo-Logdateien und Steuerdateien. Die Datenbank kann optional zu einem bestimmten Zeitpunkt wiederhergestellt werden, basierend auf den angegebenen Wiederherstellungsoptionen.



Das Klonen schlägt fehl, wenn Sie versuchen, eine auf einem Linux-Host erstellte Sicherung auf einen AIX-Host zu klonen oder umgekehrt.

SnapCenter erstellt eine eigenständige Datenbank, wenn es aus einer Oracle RAC-Datenbanksicherung geklont wird. SnapCenter unterstützt das Erstellen von Klonen aus der Sicherung einer Data Guard-Standby- und Active Data Guard-Standby-Datenbank.

Während des Klonens stellt SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf SCN oder Datum und Uhrzeit für Wiederherstellungsvorgänge bereit. Nach der Wiederherstellung wird die Protokollsicherung ausgehängt. Alle diese Klone werden unter `/var/opt/snapcenter/scu/clones/` gemountet. Wenn Sie ASM über NFS verwenden, sollten Sie `/var/opt/snapcenter/scu/clones/*/*` zum vorhandenen Pfad hinzufügen, der im Parameter `asm_diskstring` definiert ist.

Beim Klonen einer Sicherung einer ASM-Datenbank in einer SAN-Umgebung werden Udev-Regeln für die geklonten Hostgeräte unter `/etc/udev/rules.d/999-scu-netapp.rules` erstellt. Diese mit den geklonten Hostgeräten verknüpften Udev-Regeln werden gelöscht, wenn Sie den Klon löschen.



In einem Flex ASM-Setup können Sie keinen Klonvorgang auf Leaf-Knoten durchführen, wenn die Kardinalität kleiner ist als die Anzahl der Knoten im RAC-Cluster.

- 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.

## 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank entweder aus der Datenbankdetailansicht oder aus der Ressourcengruppendetailansicht aus.

Die Seite „Datenbanktopologie“ 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 die Datensicherung aus der Tabelle aus und klicken Sie dann auf \*  \*.
6. Führen Sie auf der Seite „Name“ eine der folgenden Aktionen aus:

| Wenn Sie wollen...                          | Schritte...                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Klonen einer Datenbank (CDB oder nicht CDB) | <p>a. Geben Sie die SID des Klons an.</p> <p>Die Klon-SID ist standardmäßig nicht verfügbar und die maximale Länge der SID beträgt 8 Zeichen.</p> <div>  <p>Sie sollten sicherstellen, dass auf dem Host, auf dem der Klon erstellt wird, keine Datenbank mit derselben SID vorhanden ist.</p> </div> |
| Klonen einer Pluggable-Datenbank (PDB)      | <p>a. Wählen Sie <b>PDB-Klon</b>.</p> <p>b. Geben Sie die PDB an, die Sie klonen möchten.</p> <p>c. Geben Sie den Namen der geklonten PDB an. Detaillierte Schritte zum Klonen einer PDB finden Sie unter "<a href="#">Klonen einer steckbaren Datenbank</a>".</p>                                                                                                                     |

Wenn Sie gespiegelte oder Tresordaten auswählen:

- Wenn es keine Protokollsicherung im Spiegel oder Tresor gibt, wird nichts ausgewählt und die Locatoren sind leer.
- Wenn Protokollsicherungen im Spiegel oder Tresor vorhanden sind, wird die neueste Protokollsicherung ausgewählt und der entsprechende Locator angezeigt.



Wenn die ausgewählte Protokollsicherung sowohl am Spiegel- als auch am Tresorspeicherort vorhanden ist, werden beide Locatoren angezeigt.

7. Führen Sie auf der Seite „Standorte“ die folgenden Aktionen aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Klonhost           | <p>Standardmäßig wird der Quelldatenbankhost ausgefüllt.</p> <p>Wenn Sie den Klon auf einem alternativen Host erstellen möchten, wählen Sie den Host mit derselben Oracle- und Betriebssystemversion wie der Host der Quelldatenbank.</p> |

| Für dieses Feld...                   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Speicherorte der Datendateien</p> | <p>Standardmäßig ist der Speicherort der Datendatei ausgefüllt.</p> <p>Die SnapCenter -Standardbenennungskonvention für SAN- oder NFS-Dateisysteme lautet „FileSystemNameofsourcedatabase_CLONESID“.</p> <p>Die SnapCenter -Standardbenennungskonvention für ASM-Datenträgergruppen lautet SC_HASHCODEofDISKGROUP_CLONESID. Der HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Datenträgergruppe eindeutig ist.</p> <div data-bbox="873 699 927 751">  </div> <div data-bbox="989 642 1451 808"> <p>Wenn Sie den Namen der ASM-Datenträgergruppe anpassen, stellen Sie sicher, dass die Namenslänge der von Oracle unterstützten Maximallänge entspricht.</p> </div> <p>Wenn Sie einen anderen Pfad angeben möchten, müssen Sie die Datendatei-Mount-Punkte oder ASM-Datenträgergruppennamen für die Klondatenbank eingeben. Wenn Sie den Datendateipfad anpassen, müssen Sie auch die ASM-Datenträgergruppennamen oder das Dateisystem der Steuerdatei und der Redo-Log-Datei ändern, entweder in denselben Namen wie für Datendateien oder in eine vorhandene ASM-Datenträgergruppe oder ein vorhandenes ASM-Dateisystem.</p> |

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Steuerdateien      | <p>Standardmäßig ist der Pfad der Steuerdatei ausgefüllt.</p> <p>Die Steuerdateien werden in derselben ASM-Datenträgergruppe oder demselben Dateisystem wie die Datendateien abgelegt. Wenn Sie den Steuerdateipfad überschreiben möchten, können Sie einen anderen Steuerdateipfad angeben.</p> <div data-bbox="873 495 927 552">  </div> <div data-bbox="989 474 1406 573"> <p>Das Dateisystem oder die ASM-Datenträgergruppe sollte auf dem Host vorhanden sein.</p> </div> <p>Standardmäßig entspricht die Anzahl der Steuerdateien der Anzahl der Quelldatenbank. Sie können die Anzahl der Steuerdateien ändern, zum Klonen der Datenbank ist jedoch mindestens eine Steuerdatei erforderlich.</p> <p>Sie können den Pfad der Steuerdatei an ein anderes (vorhandenes) Dateisystem als das der Quelldatenbank anpassen.</p> |



| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Redo-Protokolle    | <p>Standardmäßig werden die Redo-Log-Dateigruppe, der Pfad und ihre Größen ausgefüllt.</p> <p>Die Redo-Protokolle werden in derselben ASM-Datenträgergruppe oder demselben Dateisystem abgelegt wie die Datendateien der geklonten Datenbank. Wenn Sie den Pfad der Redo-Log-Datei überschreiben möchten, können Sie den Pfad der Redo-Log-Datei auf ein anderes Dateisystem als das der Quelldatenbank anpassen.</p> <div data-bbox="873 562 928 619">  </div> <div data-bbox="987 541 1416 640"> <p>Das neue Dateisystem oder die ASM-Datenträgergruppe sollte auf dem Host vorhanden sein.</p> </div> <p>Standardmäßig sind die Anzahl der Redo-Log-Gruppen, Redo-Log-Dateien und deren Größe identisch mit denen der Quelldatenbank. Sie können die folgenden Parameter ändern:</p> <ul style="list-style-type: none"> <li>• Anzahl der Redo-Log-Gruppen</li> </ul> <div data-bbox="873 955 928 1012">  </div> <div data-bbox="987 934 1448 1033"> <p>Zum Klonen der Datenbank sind mindestens zwei Redo-Log-Gruppen erforderlich.</p> </div> <ul style="list-style-type: none"> <li>• Redo-Logdateien in jeder Gruppe und deren Pfad</li> </ul> <p>Sie können den Pfad der Redo-Log-Datei auf ein anderes (vorhandenes) Dateisystem als das der Quelldatenbank anpassen.</p> <div data-bbox="873 1360 928 1417">  </div> <div data-bbox="987 1339 1432 1438"> <p>Zum Klonen der Datenbank ist mindestens eine Redo-Log-Datei in der Redo-Log-Gruppe erforderlich.</p> </div> <ul style="list-style-type: none"> <li>• Größen der Redo-Log-Datei</li> </ul> |

8. Führen Sie auf der Seite „Anmeldeinformationen“ die folgenden Aktionen aus:

| Für dieses Feld...                           | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationsname für den Sys-Benutzer | <p>Wählen Sie die Anmeldeinformationen aus, die zum Definieren des Sys-Benutzerkennworts der Klondatenbank verwendet werden sollen.</p> <p>Wenn SQLNET.AUTHENTICATION_SERVICES in der Datei sqlnet.ora auf dem Zielhost auf NONE gesetzt ist, sollten Sie in der SnapCenter -GUI nicht <b>None</b> als Anmeldeinformation auswählen.</p>                       |
| Name der ASM-Instanzanmeldeinformationen     | <p>Wählen Sie <b>Keine</b> aus, wenn die Betriebssystemauthentifizierung für die Verbindung mit der ASM-Instanz auf dem Klonhost aktiviert ist.</p> <p>Andernfalls wählen Sie die Oracle ASM-Anmeldeinformationen aus, die entweder mit dem Benutzer „sys“ oder einem Benutzer mit der für den Klonhost geltenden Berechtigung „sysasm“ konfiguriert sind.</p> |

Die Oracle-Home-, Benutzername- und Gruppendetails werden automatisch aus der Quelldatenbank übernommen. Sie können die Werte basierend auf der Oracle-Umgebung des Hosts ändern, auf dem der Klon erstellt wird.

9. Führen Sie auf der Seite „PreOps“ die folgenden Schritte aus:

- a. Geben Sie den Pfad und die Argumente des Präskripts ein, das Sie vor dem Klonvorgang ausführen möchten.

Sie müssen das Prescript entweder in `/var/opt/snapcenter/spl/scripts` oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad `/var/opt/snapcenter/spl/scripts` ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads abgelegt haben, müssen Sie den vollständigen Pfad bis zu dem Ordner angeben, in dem das Skript abgelegt ist.

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen. ["Mehr erfahren"](#)

- b. Ändern Sie im Abschnitt „Datenbankparametereinstellungen“ die Werte der vorab ausgefüllten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.

Sie können zusätzliche Parameter hinzufügen, indem Sie auf  klicken.  \*.

Wenn Sie Oracle Standard Edition verwenden und die Datenbank im Archivprotokollmodus ausgeführt wird oder Sie eine Datenbank aus dem Archiv-Redo-Log wiederherstellen möchten, fügen Sie die Parameter hinzu und geben Sie den Pfad an.

- LOG\_ARCHIVE\_DEST
- LOG\_ARCHIVE\_DUPLEX\_DEST



Der Fast Recovery Area (FRA) ist in den vorab ausgefüllten Datenbankparametern nicht definiert. Sie können FRA konfigurieren, indem Sie die entsprechenden Parameter hinzufügen.



Der Standardwert von log\_archive\_dest\_1 ist \$ORACLE\_HOME/clone\_sid und die Archivprotokolle der geklonten Datenbank werden an diesem Speicherort erstellt. Wenn Sie den Parameter log\_archive\_dest\_1 gelöscht haben, wird der Speicherort des Archivprotokolls von Oracle bestimmt. Sie können einen neuen Speicherort für das Archivprotokoll definieren, indem Sie log\_archive\_dest\_1 bearbeiten. Stellen Sie jedoch sicher, dass das Dateisystem oder die Datenträgergruppe vorhanden und auf dem Host verfügbar ist.

a. Klicken Sie auf **Zurücksetzen**, um die Standardeinstellungen der Datenbankparameter wiederherzustellen.

10. Auf der Seite „PostOps“ sind standardmäßig **„Datenbank wiederherstellen“** und **„Bis Abbrechen“** ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

SnapCenter führt die Wiederherstellung durch, indem es die neueste Protokollsicherung einbindet, die die ununterbrochene Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung enthält. Um den Klon auf dem Primärspeicher durchzuführen, sollten sich die Protokoll- und Datensicherung auf dem Primärspeicher befinden, und um den Klon auf dem Sekundärspeicher durchzuführen, sollten sich die Protokoll- und Datensicherung auf dem Sekundärspeicher befinden.

Die Optionen **Datenbank wiederherstellen** und **Bis Abbrechen** werden nicht ausgewählt, wenn SnapCenter die entsprechenden Protokollsicherungen nicht finden kann. Sie können den externen Archivprotokollspeicherort angeben, wenn unter **Externe Archivprotokollspeicherorte angeben** keine Protokollsicherung verfügbar ist. Sie können mehrere Protokollspeicherorte angeben.



Wenn Sie eine Quelldatenbank klonen möchten, die für die Unterstützung von Flash Recovery Area (FRA) und Oracle Managed Files (OMF) konfiguriert ist, muss das Protokollziel für die Wiederherstellung auch der OMF-Verzeichnisstruktur entsprechen.

Die Seite „PostOps“ wird nicht angezeigt, wenn es sich bei der Quelldatenbank um eine Data Guard-Standby- oder eine Active Data Guard-Standby-Datenbank handelt. Für Data Guard-Standby oder eine Active Data Guard-Standby-Datenbank bietet SnapCenter keine Option zum Auswählen des Wiederherstellungstyps in der SnapCenter -GUI, aber die Datenbank wird mit dem Wiederherstellungstyp „Bis zum Abbrechen“ wiederhergestellt, ohne dass Protokolle angewendet werden.

| Feldname      | Beschreibung                                                                                                                                                                                                                                                                                                   |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bis Abbrechen | SnapCenter führt die Wiederherstellung durch, indem es die neueste Protokollsicherung mit der ununterbrochenen Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung bereitstellt. Die geklonte Datenbank wird bis auf die fehlende oder beschädigte Protokolldatei wiederhergestellt. |

| Feldname                                           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Datum und Uhrzeit                                  | <p>SnapCenter stellt die Datenbank bis zu einem angegebenen Datum und einer angegebenen Uhrzeit wieder her. Das akzeptierte Format ist mm/tt/jjjj hh:mm:ss.</p> <div>  <p>Die Zeit kann im 24-Stunden-Format angegeben werden.</p> </div>                                                                                                                                                                                                                                     |
| Bis SCN (System Change Number)                     | <p>SnapCenter stellt die Datenbank bis zu einer angegebenen Systemänderungsnummer (SCN) wieder her.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Angeben externer Speicherorte für Archivprotokolle | <p>Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird, ermittelt und mountet SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit.</p> <p>Sie können auch den Speicherort des externen Archivprotokolls angeben.</p> <div>  <p>SnapCenter identifiziert und mountet die Protokollsicherungen nicht automatisch, wenn Sie „Bis zum Abbrechen“ ausgewählt haben.</p> </div> |
| Neue DBID erstellen                                | <p>Standardmäßig ist das Kontrollkästchen <b>Neue DBID erstellen</b> aktiviert, um eine eindeutige Nummer (DBID) für die geklonte Datenbank zu generieren, die sie von der Quelldatenbank unterscheidet.</p> <p>Deaktivieren Sie das Kontrollkästchen, wenn Sie der geklonten Datenbank die DBID der Quelldatenbank zuweisen möchten. Wenn Sie in diesem Szenario die geklonte Datenbank beim externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.</p>                                     |
| Tempfile für temporären Tablespace erstellen       | <p>Aktivieren Sie das Kontrollkästchen, wenn Sie eine temporäre Datei für den temporären Standardtabellenbereich der geklonten Datenbank erstellen möchten.</p> <p>Wenn das Kontrollkästchen nicht aktiviert ist, wird der Datenbankklon ohne die temporäre Datei erstellt.</p>                                                                                                                                                                                                                                                                                |

| Feldname                                                                          | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Geben Sie SQL-Einträge ein, die beim Erstellen des Klons angewendet werden sollen | Fügen Sie die SQL-Einträge hinzu, die Sie beim Erstellen des Klons anwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Geben Sie Skripts ein, die nach dem Klonvorgang ausgeführt werden sollen          | <p>Geben Sie den Pfad und die Argumente des Postscripts an, das Sie nach dem Klonvorgang ausführen möchten.</p> <p>Sie sollten das Postscript entweder in <code>/var/opt/snapcenter/spl/scripts</code> oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig wird der Pfad <code>/var/opt/snapcenter/spl/scripts</code> ausgefüllt.</p> <p>Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads abgelegt haben, müssen Sie den vollständigen Pfad bis zu dem Ordner angeben, in dem das Skript abgelegt ist.</p> <div>  <p>Wenn der Klonvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungsaktivitäten werden direkt ausgelöst.</p> </div> |

11. 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-SmSmtServer“ angegeben haben.

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



Während der Wiederherstellung als Teil der Klonerstellung wird der Klon mit einer Warnung erstellt, auch wenn die Wiederherstellung fehlschlägt. Sie können eine manuelle Wiederherstellung dieses Klons durchführen, um die Klondatenbank in einen konsistenten Zustand zu bringen.

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

## Ergebnis

Nach dem Klonen der Datenbank können Sie die Ressourcenseite aktualisieren, um die geklonte Datenbank als eine der für die Sicherung verfügbaren Ressourcen aufzulisten. Die geklonte Datenbank kann wie jede andere Datenbank mithilfe des Standard-Backup-Workflows geschützt oder in eine Ressourcengruppe (entweder neu erstellt oder vorhanden) aufgenommen werden. Die geklonte Datenbank kann weiter geklont werden (Klon von Klonen).

Nach dem Klonen sollten Sie die geklonte Datenbank niemals umbenennen.



Wenn Sie während des Klonens keine Wiederherstellung durchgeführt haben, kann die Sicherung der geklonten Datenbank aufgrund einer nicht ordnungsgemäßen Wiederherstellung fehlschlagen und Sie müssen möglicherweise eine manuelle Wiederherstellung durchführen. Die Protokollsicherung kann auch fehlschlagen, wenn sich der für Archivprotokolle ausgefüllte Standardspeicherort auf einem Nicht- NetApp -Speicher befindet oder wenn das Speichersystem nicht mit SnapCenter konfiguriert ist.

Im AIX-Setup können Sie den Befehl `lkdev` zum Sperren und den Befehl `rendev` zum Umbenennen der Datenträger verwenden, auf denen sich die geklonte Datenbank befand.

Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Löschvorgang des Klon. Bei auf SAN-Geräten erstellten AIX-LVM-Layouts wird das Umbenennen von Geräten für die geklonten SAN-Geräte nicht unterstützt.

### Weitere Informationen finden

- ["Wiederherstellung oder Klonen schlägt mit der Fehlermeldung ORA-00308 fehl"](#)
- ["Eine geklonte Datenbank konnte nicht wiederhergestellt werden"](#)
- ["Anpassbare Parameter für Sicherungs-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"](#)

### Aktualisieren Sie die bevorzugte IP auf dem Host

Nachdem der Klonvorgang abgeschlossen ist, liegt der vom Storage Access Layer (SAL) bereitgestellte Pfad zum Klon im Format `<nfs_lif_IP>:<JunctionPath>` vor. Um die bevorzugte IP bereitzustellen, müssen Sie sie mithilfe der SCCLI-Befehle auf dem Host konfigurieren.

#### Schritte

1. Melden Sie sich beim Datenbankhost an.
2. Initiieren Sie eine PowerShell-Verbindungssitzung mit SnapCenter für einen angegebenen Benutzer.

Öffnen-SmConnection

3. Erstellen Sie eine leere Datei.

berühren Sie `/var/opt/snapcenter/scu/etc/storagepreference.properties`

4. Konfigurieren Sie das bevorzugte Daten-LIF für die SVM.

`Add-SvmPreferredDataPath -SVM <SVM-Name> -DataPath <IP-Adresse oder FQDN>`

5. Überprüfen Sie den bevorzugten Pfad.

`Get-SvmPreferredDataPath`

### Klonen einer steckbaren Datenbank

Sie können eine Pluggable Database (PDB) auf eine andere oder dieselbe Ziel-CDB auf demselben Host oder einem alternativen Host klonen. Sie können die geklonte PDB auch zu einem gewünschten SCN oder Datum und einer gewünschten Uhrzeit wiederherstellen.

## Bevor Sie beginnen

Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

## 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 „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (mehrere Mandanten)“ entweder aus der Datenbankdetailansicht oder aus der Ressourcengruppendetailansicht aus.

Die Seite „Datenbanktopologie“ 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 „Name“ die folgenden Aktionen aus:
  - a. Wählen Sie **PDB-Klon**.
  - b. Geben Sie die PDB an, die Sie klonen möchten.



Sie können jeweils nur eine PDB klonen.

- c. Geben Sie den Namen der geklonten PDB an.

7. Führen Sie auf der Seite „Standorte“ die folgenden Aktionen aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Klonhost           | <p>Standardmäßig wird der Quelldatenbankhost ausgefüllt.</p> <p>Wenn Sie den Klon auf einem alternativen Host erstellen möchten, wählen Sie den Host mit derselben Oracle- und Betriebssystemversion wie der Host der Quelldatenbank.</p> |
| Ziel-CDB           | <p>Wählen Sie die CDB aus, in die Sie die geklonte PDB einfügen möchten.</p> <p>Sie sollten sicherstellen, dass die Ziel-CDB ausgeführt wird.</p>                                                                                         |
| Datenbankstatus    | <p>Aktivieren Sie das Kontrollkästchen <b>Öffnen Sie die geklonte PDB im LESE-/SCHREIB-Modus</b>, wenn Sie die PDB im LESE-/SCHREIB-Modus öffnen möchten.</p>                                                                             |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Speicherorte der Datendateien</p> | <p>Standardmäßig ist der Speicherort der Datendatei ausgefüllt.</p> <p>Die SnapCenter -Standardbenennungskonvention für SAN- oder NFS-Dateisysteme lautet „FileSystemNameofsourcedatabase_SCJOBID“.</p> <p>Die SnapCenter -Standardbenennungskonvention für ASM-Datenträgergruppen lautet SC_HASHCODEofDISKGROUP_SCJOBID. Der HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Datenträgergruppe eindeutig ist.</p> <div data-bbox="873 642 927 695">  </div> <p>Wenn Sie den Namen der ASM-Datenträgergruppe anpassen, stellen Sie sicher, dass die Namenslänge der von Oracle unterstützten Maximallänge entspricht.</p> <p>Wenn Sie einen anderen Pfad angeben möchten, müssen Sie die Datendatei-Mount-Punkte oder ASM-Datenträgergruppennamen für die Klondatenbank eingeben.</p> |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Die Oracle-Home-, Benutzername- und Gruppendetails werden automatisch aus der Quelldatenbank übernommen. Sie können die Werte basierend auf der Oracle-Umgebung des Hosts ändern, auf dem der Klon erstellt wird.

8. Führen Sie auf der Seite „PreOps“ die folgenden Schritte aus:

- a. Geben Sie den Pfad und die Argumente des Präskripts ein, das Sie vor dem Klonvorgang ausführen möchten.

Sie sollten das Prescript entweder in /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner innerhalb dieses Pfads speichern. Standardmäßig ist der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads abgelegt haben, müssen Sie den vollständigen Pfad bis zu dem Ordner angeben, in dem das Skript abgelegt ist.

SnapCenter ermöglicht Ihnen die Verwendung der vordefinierten Umgebungsvariablen, wenn Sie das Prescript und Postscript ausführen. ["Mehr erfahren"](#)

- a. Ändern Sie im Abschnitt „Einstellungen der Hilfsdatenbankparameter für CDB-Klone“ die Werte der vorab ausgefüllten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.

9. Klicken Sie auf **Zurücksetzen**, um die Standardeinstellungen der Datenbankparameter wiederherzustellen.
10. Auf der Seite „PostOps“ ist standardmäßig **„Bis Abbrechen“** ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

Die Option **Bis Abbrechen** wird nicht ausgewählt, wenn SnapCenter die entsprechenden Protokollsicherungen nicht finden kann. Sie können den externen Archivprotokollspeicherort angeben, wenn unter **Externe Archivprotokollspeicherorte angeben** keine Protokollsicherung verfügbar ist. Sie



können mehrere Protokollspeicherorte angeben.



Wenn Sie eine Quelldatenbank klonen möchten, die für die Unterstützung von Flash Recovery Area (FRA) und Oracle Managed Files (OMF) konfiguriert ist, muss das Protokollziel für die Wiederherstellung auch der OMF-Verzeichnisstruktur entsprechen.

| Feldname                                           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bis Abbrechen                                      | <p>SnapCenter führt die Wiederherstellung durch, indem es die neueste Protokollsicherung mit der ununterbrochenen Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung bereitstellt.</p> <p>Um den Klon auf dem Primärspeicher durchzuführen, sollten sich die Protokoll- und Datensicherung auf dem Primärspeicher befinden, und um den Klon auf dem Sekundärspeicher durchzuführen, sollten sich die Protokoll- und Datensicherung auf dem Sekundärspeicher befinden. Die geklonte Datenbank wird bis auf die fehlende oder beschädigte Protokolldatei wiederhergestellt.</p> |
| Datum und Uhrzeit                                  | <p>SnapCenter stellt die Datenbank bis zu einem angegebenen Datum und einer angegebenen Uhrzeit wieder her.</p> <div> Die Zeit kann im 24-Stunden-Format angegeben werden.</div>                                                                                                                                                                                                                                                                                                                                      |
| Bis SCN (System Change Number)                     | <p>SnapCenter stellt die Datenbank bis zu einer angegebenen Systemänderungsnummer (SCN) wieder her.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Angeben externer Speicherorte für Archivprotokolle | <p>Geben Sie den Speicherort des externen Archivprotokolls an.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Neue DBID erstellen                                | <p>Standardmäßig ist das Kontrollkästchen <b>Neue DBID erstellen</b> für die Hilfsklondatenbank nicht aktiviert.</p> <p>Aktivieren Sie das Kontrollkästchen, wenn Sie für die geklonte Hilfsdatenbank eine eindeutige Nummer (DBID) generieren möchten, die sie von der Quelldatenbank unterscheidet.</p>                                                                                                                                                                                                                                                                                                |

| Feldname                                                                          | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tempfile für temporären Tablespace erstellen                                      | <p>Aktivieren Sie das Kontrollkästchen, wenn Sie eine temporäre Datei für den temporären Standardtabellenbereich der geklonten Datenbank erstellen möchten.</p> <p>Wenn das Kontrollkästchen nicht aktiviert ist, wird der Datenbankklon ohne die temporäre Datei erstellt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Geben Sie SQL-Einträge ein, die beim Erstellen des Klons angewendet werden sollen | Fügen Sie die SQL-Einträge hinzu, die Sie beim Erstellen des Klons anwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Geben Sie Skripts ein, die nach dem Klonvorgang ausgeführt werden sollen          | <p>Geben Sie den Pfad und die Argumente des Postscripts an, das Sie nach dem Klonvorgang ausführen möchten.</p> <p>Sie sollten das Postscript entweder in <code>/var/opt/snapcenter/spl/scripts</code> oder in einem beliebigen Ordner innerhalb dieses Pfads speichern.</p> <p>Standardmäßig wird der Pfad <code>/var/opt/snapcenter/spl/scripts</code> ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads abgelegt haben, müssen Sie den vollständigen Pfad bis zu dem Ordner angeben, in dem das Skript abgelegt ist.</p> <div>  <p>Wenn der Klonvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungsaktivitäten werden direkt ausgelöst.</p> </div> |

11. 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-SmSmtServer“ angegeben haben.

12. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
13. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

### Nachdem Sie fertig sind

Wenn Sie eine Sicherung der geklonten PDB erstellen möchten, sollten Sie die Ziel-CDB sichern, in der die PDB geklont wird, da es nicht möglich ist, nur die geklonte PDB zu sichern. Sie sollten eine sekundäre

Beziehung für die Ziel-CDB erstellen, wenn Sie das Backup mit sekundärer Beziehung erstellen möchten.

In einem RAC-Setup wird der Speicher für geklonte PDBs nur an den Knoten angeschlossen, auf dem der PDB-Klon durchgeführt wurde. Die PDBs auf den anderen Knoten des RAC befinden sich im MOUNT-Status. Wenn Sie möchten, dass die geklonte PDB von den anderen Knoten aus zugänglich ist, sollten Sie den Speicher manuell an die anderen Knoten anhängen.

### Weitere Informationen finden

- ["Wiederherstellung oder Klonen schlägt mit der Fehlermeldung ORA-00308 fehl"](#)
- ["Anpassbare Parameter für Sicherungs-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"](#)

## Klonen Sie Oracle-Datenbanksicherungen mit UNIX-Befehlen

Der Klon-Workflow umfasst die Planung, Durchführung und Überwachung des Klonvorgangs.

### Über diese Aufgabe

Sie sollten die folgenden Befehle ausführen, um die Spezifikationsdatei für den Oracle-Datenbankklon zu erstellen und den Klonvorgang zu starten.

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"](#) .

### Schritte

1. Erstellen Sie eine Oracle-Datenbank-Klonspezifikation aus einem angegebenen Backup: *New-SmOracleCloneSpecification*



Wenn die sekundäre Datenschutzrichtlinie ein einheitlicher Spiegeltresor ist, geben Sie nur `-IncludeSecondaryDetails` an. Sie müssen `-SecondaryStorageType` nicht angeben.

Dieser Befehl erstellt automatisch eine Oracle-Datenbank-Klonspezifikationsdatei für die angegebene Quelldatenbank und deren Sicherung. Sie müssen außerdem eine SID für die Klondatenbank angeben, damit die erstellte Spezifikationsdatei die automatisch generierten Werte für die von Ihnen erstellte Klondatenbank enthält.



Die Klonspezifikationsdatei wird unter `/var/opt/snapcenter/sco/clone_specs` erstellt.

2. Starten Sie einen Klonvorgang aus einer Klonressourcengruppe oder einem vorhandenen Backup: *New-SmClone*

Dieser Befehl leitet einen Klonvorgang ein. Sie müssen außerdem einen Oracle-Klonspezifikationsdateipfad für den Klonvorgang angeben. Sie können auch die Wiederherstellungsoptionen, den Host, auf dem der Klonvorgang ausgeführt werden soll, Präskripte, Postskripte und andere Details angeben.

Standardmäßig wird die Zielfeile des Archivprotokolls für die Klondatenbank automatisch unter `$ORACLE_HOME/CLONE_SIDs` ausgefüllt.

## Aufteilen eines Oracle-Datenbankklons

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

### Über diese Aufgabe

- 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 teilen, werden die Sicherungskopien des Klons gelöscht.
- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["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“ in der Liste „Ansicht“ die Option „Datenbank“ aus.
3. Wählen Sie die geklonte Ressource (z. B. die Datenbank oder LUN) aus und klicken Sie dann auf  .
4. Überprüfen Sie die geschätzte Größe des aufzuteilenden Klons und den erforderlichen verfügbaren Speicherplatz auf dem Aggregat und klicken Sie dann auf **Start**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

Der Klon-Split-Vorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird und die Datenbanken, für die der Klon-Split-Vorgang durchgeführt wurde, auf der Seite „Ressourcen“ als Klone aufgeführt werden. 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.

Zum Beispiel,

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



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

## Geteilter Klon einer steckbaren Datenbank

Sie können SnapCenter verwenden, um eine geklonte Pluggable Database (PDB) aufzuteilen.

### Über diese Aufgabe

Wenn Sie eine Sicherung der Ziel-CDB erstellt haben, in der die PDB geklont ist, wird beim Aufteilen des PDB-Klons die geklonte PDB auch aus allen Sicherungen der Ziel-CDB entfernt, die die geklonte PDB enthalten.



Die PDB-Klone werden nicht in der Inventar- oder Ressourcenansicht angezeigt.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie die Quellcontainerdatenbank (CDB) aus der Ressourcen- oder Ressourcengruppenansicht aus.
3. Wählen Sie in der Ansicht „Kopien verwalten“ **Klone** entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
4. Wählen Sie den PDB-Klon (targetCDB:PDBClone) 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.

## Überwachen von Oracle-Datenbankklonvorgängen

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**.

## Aktualisieren eines Klons

Sie können den Klon aktualisieren, indem Sie den Befehl *Refresh-SmClone* ausführen. Dieser Befehl erstellt eine Sicherungskopie der Datenbank, löscht den vorhandenen Klon und erstellt einen Klon mit demselben Namen.



Sie können einen PDB-Klon nicht aktualisieren.

### Was Sie brauchen

- Erstellen Sie eine vollständige Onlinesicherung oder eine Offline-Datensicherungsrichtlinie ohne aktivierte geplante Sicherungen.
- Konfigurieren Sie die E-Mail-Benachrichtigung in der Richtlinie nur für Sicherheitsfehler.
- Definieren Sie die Aufbewahrungsdauer für die On-Demand-Backups entsprechend, um sicherzustellen, dass keine unerwünschten Backups erstellt werden.
- Stellen Sie sicher, dass der Ressourcengruppe, die für den Aktualisierungsklonvorgang identifiziert wurde, nur eine Online-Vollsicherung oder eine Offline-Datensicherungsrichtlinie zugeordnet ist.
- Erstellen Sie eine Ressourcengruppe mit nur einer Datenbank.
- Wenn für den Befehl zum Aktualisieren des Klons ein Cron-Job erstellt wird, stellen Sie sicher, dass sich die SnapCenter -Zeitpläne und die Cron-Zeitpläne für die Datenbankressourcengruppe nicht überschneiden.

Stellen Sie bei einem Cron-Job, der für den Befehl zum Aktualisieren des Klons erstellt wurde, sicher, dass Sie alle 24 Stunden Open-SmConnection ausführen.

- Stellen Sie sicher, dass die Klon-SID für einen Host eindeutig ist.

Wenn mehrere Aktualisierungsklonvorgänge dieselbe Klonspezifikationsdatei verwenden oder die Klonspezifikationsdatei mit derselben Klon-SID verwenden, wird der vorhandene Klon mit der SID auf dem Host gelöscht und anschließend der Klon erstellt.

- Stellen Sie sicher, dass die Sicherungsrichtlinie mit sekundärem Schutz aktiviert ist und die Klonspezifikationsdatei mit „IncludeSecondaryDetails“ erstellt wird, um die Klone mithilfe sekundärer Sicherungen zu erstellen.
  - Wenn die primäre Klonspezifikationsdatei angegeben ist, in der Richtlinie jedoch die sekundäre

Updateoption ausgewählt ist, wird die Sicherung erstellt und das Update auf die sekundäre Datei übertragen. Der Klon wird jedoch aus der primären Sicherung erstellt.

- Wenn die primäre Klon spezifikationsdatei angegeben ist und in der Richtlinie keine sekundäre Aktualisierungsoption ausgewählt ist, wird die Sicherung auf dem Primärserver erstellt und der Klon wird vom Primärserver erstellt.

## Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer: *Open-SmConnection*
2. Erstellen Sie eine Oracle-Datenbank-Klon spezifikation aus einem angegebenen Backup: *New-SmOracleCloneSpecification*



Wenn die sekundäre Datenschutzrichtlinie ein einheitlicher Spiegeltresor ist, geben Sie nur `-IncludeSecondaryDetails` an. Sie müssen `-SecondaryStorageType` nicht angeben.

Dieser Befehl erstellt automatisch eine Oracle-Datenbank-Klon spezifikationsdatei für die angegebene Quelldatenbank und deren Sicherung. Sie müssen außerdem eine SID für die Klondatenbank angeben, damit die erstellte Spezifikationsdatei die automatisch generierten Werte für die von Ihnen erstellte Klondatenbank enthält.



Die Klon spezifikationsdatei wird unter `/var/opt/snapcenter/sco/clone_specs` erstellt.

3. Führen Sie *Refresh-SmClone* aus.

Wenn der Vorgang mit der Fehlermeldung „PL-SCO-20032: canExecute-Vorgang ist mit Fehler fehlgeschlagen: PL-SCO-30031: Redo-Protokolldatei +SC\_2959770772\_clmdb/clmdb/redolog/redo01\_01.log vorhanden“ fehlschlägt, geben Sie einen höheren Wert für `-WaitToTriggerClone` an.

Ausführliche Informationen zu UNIX-Befehlen finden Sie im ["SnapCenter Software-Befehlsreferenzhandbuch"](#).

## Klon einer Pluggable-Datenbank löschen

Sie können den Klon einer Pluggable-Datenbank (PDB) löschen, wenn Sie ihn nicht mehr benötigen.

Wenn Sie eine Sicherung der Ziel-CDB erstellt haben, in der die PDB geklont ist, wird beim Löschen des PDB-Klons die geklonte PDB auch aus der Sicherung der Ziel-CDB entfernt.



Die PDB-Klone werden nicht in der Inventar- oder Ressourcenansicht angezeigt.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie die Quellcontainerdatenbank (CDB) aus der Ressourcen- oder Ressourcengruppenansicht aus.
3. Wählen Sie in der Ansicht „Kopien verwalten“ **Klone** entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.

4. Wählen Sie den PDB-Klon (targetCDB:PDBClone) aus und klicken Sie dann auf  .
5. Klicken Sie auf **OK**.

## Verwalten von Anwendungsvolumes

### Was sind Anwendungsvolumina

Anwendungsvolumes sind der Speicher, in dem Informationen wie Konfigurations-, Installations- und andere Nicht-Datendateien im Zusammenhang mit der Oracle-Datenbank gespeichert werden.

Mit dem SnapCenter -Plug-in für Oracle-Datenbanken können Sie konsistente Backups von Anwendungsvolumes (keine Datenvolumes) zusammen mit den Oracle-Datenbanken erstellen.

Das Plug-in automatisiert die Sicherung und das Klonen von Anwendungsvolumes.

- Schützen Sie Anwendungsvolumes zusammen mit Oracle-Datenbankvolumes in einer einzigen Ressourcengruppe.
- Erstellen Sie Backups von Anwendungsvolumes.
- Erstellen Sie Backups von Oracle-Datenbanken zusammen mit Anwendungsvolumes.
- Erstellen Sie Klone von Datenbanken zusammen mit Anwendungsvolumes bis zu einem bestimmten Zeitpunkt.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie alle Vorgänge.
- Zeigen Sie Berichte zu Sicherungs- und Klonvorgängen an.

### Anwendungsvolumes hinzufügen

SnapCenter unterstützt das Sichern und Klonen von Anwendungsvolumes der Oracle-Datenbank. Sie sollten die Anwendungsvolumes manuell hinzufügen. Die automatische Erkennung von Anwendungsvolumes wird nicht unterstützt.



Anwendungsvolumes unterstützen nur direkte NFS- und direkte iSCSI-Verbindungen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
2. Klicken Sie auf **Anwendungsvolume hinzufügen**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:
  - Geben Sie im Feld „Name“ den Namen des Anwendungsvolumes ein.
  - Geben Sie im Feld „Hostname“ den Namen des Hosts ein.
4. Geben Sie auf der Seite „Storage Footprint“ den Namen des Speichersystems ein, wählen Sie ein oder mehrere Volumes aus und geben Sie die zugehörigen LUNs oder Qtrees an.

Sie können mehrere Speichersysteme hinzufügen.



5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
6. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolume“ aus, um alle von Ihnen hinzugefügten Anwendungsvolumen anzuzeigen.

## Anwendungslautstärke ändern

Sie können alle Werte ändern, die Sie beim Hinzufügen des Anwendungsvolumen angegeben haben, wenn keine Sicherungen erstellt werden. Wenn die Sicherung erstellt ist, können Sie nur die Details des Speichersystems ändern.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolumen“ aus.
3.  , um die Werte zu ändern.
4.  , um die Werte zu ändern.

## Anwendungsvolume löschen

Wenn Sie ein Anwendungsvolume löschen und dem Anwendungsvolume Sicherungen zugeordnet sind, wird das Anwendungsvolume in den Wartungsmodus versetzt und es werden keine neuen Sicherungen erstellt und keine früheren Sicherungen beibehalten. Wenn keine Sicherungen zugeordnet sind, werden alle Metadaten gelöscht.

Bei Bedarf können Sie den Löschvorgang mit SnapCenter rückgängig machen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolumen“ aus.
3. Klicken  Löschen-Symbol], um die Werte zu ändern.

## Backup-Anwendungsvolumen

### Anwendungsvolume sichern

Wenn das Anwendungsvolume nicht Teil einer Ressourcengruppe ist, können Sie das Anwendungsvolume von der Seite „Ressourcen“ aus sichern.

### Über diese Aufgabe

Standardmäßig werden Konsistenzgruppen-Sicherungen (CG) erstellt. Wenn Sie Volume-basierte Backups erstellen möchten, sollten Sie den Wert von **EnableOracleNdvVolumeBasedBackup** in der Datei *web.config* auf „true“ setzen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolumen“ aus.
3. Klicken Sie auf \*  \* und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern.

Sie können dann auf \* klicken:  \*, um den Filterbereich zu schließen.

4. Wählen Sie das Anwendungsvolumen aus, das Sie sichern möchten.

Die Seite „Anwendungsvolumen schützen“ wird angezeigt.

5. Führen Sie auf der Seite „Ressource“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | Aktivieren Sie dieses Kontrollkästchen und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.<br><br>Beispielsweise customtext__policy_hostname oder resource_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt. |
| Archivprotokollziele von der Sicherung ausschließen           | Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.                                                                                                                                                                                                                |

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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

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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

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

7. 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 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 „Set-SmSmtServer“ angegeben haben.

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

Die Seite mit der Anwendungsvolume-Topologie wird angezeigt.

9. Klicken Sie auf **Jetzt sichern**.

10. 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.
- b. Klicken Sie auf **Sichern**.

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

### Sichern der Anwendungsvolume-Ressourcengruppe

Sie können die Ressourcengruppe sichern, die nur Anwendungsvolumen oder eine Mischung aus Anwendungsvolumen und Datenbank enthält. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

Wenn die Ressourcengruppe über mehrere Anwendungsvolumen verfügt, sollten alle Anwendungsvolumen entweder über die Replikationsrichtlinie SnapMirror oder SnapVault verfügen.

### Über diese Aufgabe

Standardmäßig werden Konsistenzgruppen-Sicherungen (CG) erstellt. Wenn Sie Volume-basierte Backups erstellen möchten, sollten Sie den Wert von **EnableOracleNdvVolumeBasedBackup** in der Datei *web.config* auf „true“ setzen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf \* klicken.  \* und wählen Sie dann das Tag aus. Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
  - a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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 Zeitplan

angegebenen Aufbewahrungseinstellungen aufbewahrt.

b. Klicken Sie auf **Sichern**.

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



Der Überprüfungsvorgang wird nur für die Datenbanken und nicht für die Anwendungsvolumes durchgeführt.

## Klonen Sie die Datenträgersicherung der Anwendung

Sie können SnapCenter verwenden, um die Anwendungsvolume-Backups zu klonen.

### Bevor Sie beginnen

Wenn Sie das Plug-In als Nicht-Root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen für die Verzeichnisse „prescript“ und „postscript“ manuell zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolumen“ aus.
3. Wählen Sie das Anwendungsvolume entweder aus der Detailansicht des Anwendungsvolumes oder aus der Detailansicht der Ressourcengruppe aus.

Die Seite mit der Anwendungsvolume-Topologie 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...                                          |
|------------------------|------------------------------------------------------------------|
| Plug-in-Host           | Wählen Sie den Host aus, auf dem Sie den Klon erstellen möchten. |
| Name der Zielressource | Geben Sie den Ressourcennamen an.                                |

7. Geben Sie auf der Seite „Skripte“ die Namen der Skripte an, die vor dem Klonen ausgeführt werden sollen, Befehle zum Mounten eines Dateisystems und die Namen der Skripte, die nach dem Klonen ausgeführt werden sollen.
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-SmSmtServer“ angegeben haben.

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

### Aufteilen eines Anwendungsvolume-Klons

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

#### Schritte

- Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
- Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolumen“ aus.
- Wählen Sie die geklonte Ressource aus und klicken Sie auf .
- Überprüfen Sie die geschätzte Größe des aufzuteilenden Klons und den erforderlichen verfügbaren Speicherplatz auf dem Aggregat und klicken Sie dann auf **Start**.
- Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

### Löschen eines Anwendungsvolume-Klons

Sie können Klone löschen, wenn Sie sie nicht mehr benötigen. Sie können keine Klone löschen, die als Quelle für andere Klone fungieren.

#### Schritte

- Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Database-Plug-In aus der Liste aus.
- Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Anwendungsvolumen“ aus.
- Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

- Wählen Sie in der Ansicht „Kopien verwalten“ **Klone** entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
- Wählen Sie den Klon aus und klicken Sie dann auf .
- Führen Sie auf der Seite „Klon löschen“ die folgenden Aktionen aus:
  - Geben Sie im Feld **Pre clone delete** die Namen der Skripte ein, die vor dem Löschen des Klons ausgeführt werden sollen.
  - Geben Sie im Feld **Unmount** die Befehle zum Unmounten des Klons ein, bevor Sie ihn löschen.
- Klicken Sie auf **OK**.

# Schützen Sie Windows-Dateisysteme

## SnapCenter Plug-in für Microsoft Windows-Konzepte

### Übersicht über das SnapCenter -Plug-in für Microsoft Windows

Das SnapCenter -Plug-in für Microsoft Windows ist eine hostseitige Komponente der NetApp SnapCenter -Software, die eine anwendungsbewusste Datenschutzverwaltung von Microsoft-Dateisystemressourcen ermöglicht. Darüber hinaus bietet es Speicherbereitstellung, Snapshot-Konsistenz und Speicherplatzrückgewinnung für Windows-Dateisysteme. Das Plug-in für Windows automatisiert Sicherungs-, Wiederherstellungs- und Klonvorgänge des Dateisystems in Ihrer SnapCenter -Umgebung.

Wenn das Plug-in für Windows installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und mit der NetApp SnapVault -Technologie eine Disk-to-Disk-Sicherungsreplikation zur Archivierung oder Standardkonformität durchführen.

- Ermöglicht anwendungsbezogenen Datenschutz für andere Plug-Ins, die auf Windows-Hosts in Ihrer SnapCenter -Umgebung ausgeführt werden
- Automatisiert anwendungsorientierte Sicherungs-, Wiederherstellungs- und Klonvorgänge für Microsoft-Dateisysteme in Ihrer SnapCenter Umgebung
- Unterstützt Speicherbereitstellung, Snapshot-Konsistenz und Speicherplatzrückgewinnung für Windows-Hosts



Das Plug-in für Windows stellt SMB-Freigaben und Windows-Dateisysteme auf physischen und RDM-LUNs bereit, unterstützt jedoch keine Sicherungsvorgänge für Windows-Dateisysteme auf SMB-Freigaben.

### Was Sie mit dem SnapCenter Plug-in für Microsoft Windows tun können

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

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



Das Plug-in für Windows unterstützt keine Sicherung und Wiederherstellung von Dateisystemen auf SMB-Freigaben.

## Funktionen des SnapCenter -Plug-ins für Windows

Das Plug-in für Windows lässt sich in die NetApp Snapshot-Technologie auf dem Speichersystem integrieren. Um mit dem Plug-in für Windows zu arbeiten, verwenden Sie die SnapCenter -Schnittstelle.

Das Plug-in für Windows umfasst die folgenden Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche mit SnapCenter**

Die SnapCenter Schnittstelle bietet Ihnen Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs- und Wiederherstellungsprozesse über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen. SnapCenter bietet außerdem eine zentrale Planung und Richtlinienverwaltung zur Unterstützung von Sicherungs- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

Sie können routinemäßige Dateisystemsicherungen planen, eine richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge einrichten. Sie können Ihre Dateisystemumgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Technologie**

Das Plug-in für Windows verwendet die NetApp Snapshot-Technologie. Auf diese Weise können Sie Dateisysteme in Sekundenschnelle sichern und schnell wiederherstellen, ohne den Host offline zu nehmen. Snapshots verbrauchen nur minimalen Speicherplatz.

Zusätzlich zu diesen Hauptfunktionen bietet das Plug-in für Windows die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung
- Erstellung platzsparender Kopien von Produktionsdateisystemen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Informationen zur FlexClone -Lizenzierung finden Sie unter ["SnapCenter -Lizenzen"](#).

- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Servern auszuführen
- PowerShell-Cmdlets zum Skripting von Sicherungs-, Wiederherstellungs- und Klonvorgängen
- Unterstützung für die Sicherung von Dateisystemen und virtuellen Maschinendatenträgern (VMDKs)
- Unterstützung für physische und virtualisierte Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK über NFS und VMFS sowie virtuelles FC
- Unterstützung für Non-Volatile Memory Express (NVMe) auf Windows Server 2022
  - Sicherungs-, Wiederherstellungs-, Klon- und Überprüfungs-Workflows auf VMDK-Layout, das auf NVMe über TCP/IP erstellt wurde.
  - Unterstützt NVMe-Firmwareversion 1.3 ab ESX 8.0 Update 2 und erfordert virtuelle Hardwareversion 21.

- Windows Server Failover Clustering (WSFC) wird für Anwendungen über VMDK auf NVMe über TCP/IP nicht unterstützt.
- Unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie transparent ausfallen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

## So sichert SnapCenter Windows-Dateisysteme

SnapCenter verwendet Snapshot-Technologie zum Sichern von Windows-Dateisystemressourcen, die sich auf LUNs, CSVs (Cluster Shared Volumes), RDM-Volumes (Raw Device Mapping), ALM (asymmetric LUN Mapping) in Windows-Clustern und VMDKs basierend auf VMFS/NFS (VMware Virtual Machine File System using NFS) befinden.

SnapCenter erstellt Backups, indem es Snapshots der Dateisysteme erstellt. Föderierte Backups, bei denen ein Volume LUNs von mehreren Hosts enthält, sind schneller und effizienter als Backups jeder einzelnen LUN, da nur ein Snapshot des Volumes erstellt wird, im Gegensatz zu einzelnen Snapshots jedes Dateisystems.

Wenn SnapCenter einen Snapshot erstellt, wird das gesamte Speichersystemvolume im Snapshot erfasst. Allerdings ist die Sicherung nur für den Hostserver gültig, für den die Sicherung erstellt wurde.

Wenn sich Daten von anderen Hostservern auf demselben Volume befinden, können diese Daten nicht aus dem Snapshot wiederhergestellt werden.



Wenn ein Windows-Dateisystem eine Datenbank enthält, ist das Sichern des Dateisystems nicht dasselbe wie das Sichern der Datenbank. Um eine Datenbank zu sichern, müssen Sie eines der Datenbank-Plug-ins verwenden.

## Vom SnapCenter Plug-in für Microsoft Windows unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen als auch auf virtuellen Maschinen. Sie müssen überprüfen, ob für Ihren Speichertyp Unterstützung verfügbar ist, bevor Sie das Paket für Ihren Host installieren.

SnapCenter -Bereitstellungs- und Datenschutzunterstützung ist auf Windows Server verfügbar. Die neuesten Informationen zu unterstützten Versionen finden Sie im [https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp Interoperabilitätsmatrix-Tool\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\).

| Maschine          | Speichertyp                | Bereitstellung mittels                                                    | Support-Hinweise |
|-------------------|----------------------------|---------------------------------------------------------------------------|------------------|
| Physischer Server | FC-verbundene LUNs         | Grafische Benutzeroberfläche (GUI) von SnapCenter oder PowerShell-Cmdlets |                  |
| Physischer Server | Über iSCSI verbundene LUNs | SnapCenter -GUI oder PowerShell-Cmdlets                                   |                  |



| <b>Maschine</b>   | <b>Speichertyp</b>                                                                    | <b>Bereitstellung mittels</b>           | <b>Support-Hinweise</b>             |
|-------------------|---------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------|
| Physischer Server | SMB3 (CIFS)-Freigaben auf einer Storage Virtual Machine (SVM)                         | SnapCenter -GUI oder PowerShell-Cmdlets | Support nur für die Bereitstellung. |
| VMware VM         | Über einen FC- oder iSCSI-HBA verbundene RDM-LUNs                                     | PowerShell-Cmdlets                      |                                     |
| VMware VM         | iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind          | SnapCenter -GUI oder PowerShell-Cmdlets |                                     |
| VMware VM         | Virtual Machine File Systems (VMFS) oder NFS-Datenspeicher                            | VMware vSphere                          |                                     |
| VMware VM         | Ein Gastsystem, das mit SMB3-Freigaben verbunden ist, die sich auf einer SVM befinden | SnapCenter -GUI oder PowerShell-Cmdlets | Support nur für die Bereitstellung. |
| VMware VM         | vVol-Datenspeicher auf NFS und SAN                                                    | ONTAP Tools für VMware vSphere          |                                     |

| Maschine   | Speichertyp                                                                             | Bereitstellung mittels                  | Support-Hinweise                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hyper-V-VM | Virtuelle FC (vFC) LUNs, die durch einen virtuellen Fibre Channel Switch verbunden sind | SnapCenter -GUI oder PowerShell-Cmdlets | <p>Sie müssen Hyper-V Manager verwenden, um Virtual FC (vFC)-LUNs bereitzustellen, die über einen virtuellen Fibre Channel-Switch verbunden sind.</p> <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div> |
| Hyper-V-VM | iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind            | SnapCenter -GUI oder PowerShell-Cmdlets | <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div>                                                                                                                                                     |

| Maschine   | Speichertyp                                                                           | Bereitstellung mittels                  | Support-Hinweise                                                                                                                                                                                                                                                                                        |
|------------|---------------------------------------------------------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hyper-V-VM | Ein Gastsystem, das mit SMB3-Freigaben verbunden ist, die sich auf einer SVM befinden | SnapCenter -GUI oder PowerShell-Cmdlets | <p>Support nur für die Bereitstellung.</p> <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div> |

## Für das Windows-Plug-In sind mindestens ONTAP -Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN löschen
  - lun igroup hinzufügen
  - lun igroup erstellen
  - LUN-Igroup löschen
  - LUN-Igroup umbenennen
  - lun igroup show
  - LUN-Zuordnung Add-Reporting-Nodes
  - LUN-Zuordnung erstellen
  - LUN-Zuordnung löschen
  - LUN-Zuordnung zum Entfernen von Berichtsknoten

- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen

- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle anzeigen
  - vServer

## **Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation**

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär > Spiegel > Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#) .

## Definieren Sie eine Sicherungsstrategie für Windows-Dateisysteme

Durch die Definition einer Sicherungsstrategie vor der Erstellung Ihrer Sicherungen erhalten Sie die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Dateisysteme benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

### Sicherungszeitpläne für Windows-Dateisysteme

Die Sicherungshäufigkeit wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können beispielsweise die Sicherungshäufigkeit auf stündlich, täglich, wöchentlich oder monatlich konfigurieren oder „Keine“

angeben, wodurch die Richtlinie zu einer Nur-On-Demand-Richtlinie wird. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen > Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen > Ressourcengruppen** klicken.

## Anzahl der für Windows-Dateisysteme benötigten Sicherungen

Zu den Faktoren, die die Anzahl der benötigten Sicherungen bestimmen, gehören die Größe des Windows-Dateisystems, die Anzahl der verwendeten Volumes, die Änderungsrate des Dateisystems und Ihr Service Level Agreement (SLA).

## Sicherungsnamenskonvention für Windows-Dateisysteme

Für die Sicherung von Windows-Dateisystemen wird die standardmäßige Snapshot-Benennungskonvention verwendet. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standard-Namenskonvention:  
Ressourcengruppenname\_Hostname\_Zeitstempel

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- `dts1` ist der Name der Ressourcengruppe.
- `mach1x88` ist der Hostname.
- `03-12-2016\_23.17.26` ist das Datum und der Zeitstempel.

Beim Erstellen einer Sicherung können Sie auch ein beschreibendes Tag hinzufügen, um die Identifizierung der Sicherung zu erleichtern. Wenn Sie dagegen eine benutzerdefinierte Namenskonvention für die Sicherung verwenden möchten, müssen Sie die Sicherung nach Abschluss des Sicherungsvorgangs umbenennen.

## Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.



Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

## Quellen und Ziele von Klonen für Windows-Dateisysteme

Sie können eine Dateisystemsicherung vom Primär- oder Sekundärspeicher klonen. Sie können auch das Ziel auswählen, das Ihren Anforderungen entspricht: entweder den ursprünglichen Sicherungsspeicherort oder ein anderes Ziel auf demselben oder einem anderen Host. Das Ziel muss sich auf demselben Datenträger wie die Klon-Quellsicherung befinden.

| Klonziel                   | Beschreibung                                                                                                                                                                                    |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original, Quelle, Standort | Standardmäßig speichert SnapCenter den Klon am selben Ort und auf demselben Host wie das zu klonende Backup.                                                                                    |
| Anderer Standort           | Sie können den Klon an einem anderen Ort auf demselben Host oder auf einem anderen Host speichern. Der Host muss über eine konfigurierte Verbindung zur Storage Virtual Machine (SVM) verfügen. |

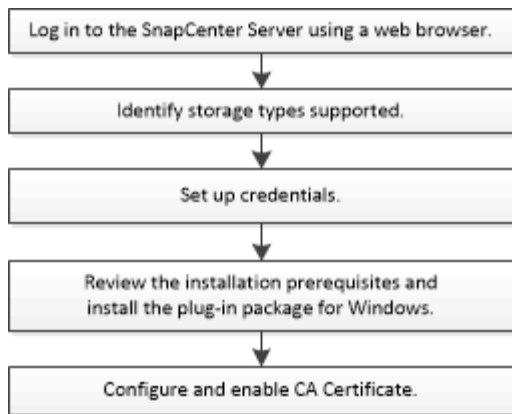
Sie können den Klon umbenennen, nachdem der Klonvorgang abgeschlossen ist.

## Installieren Sie das SnapCenter -Plug-in für Microsoft Windows

### Installationsablauf des SnapCenter Plug-ins für Microsoft Windows

Sie müssen das SnapCenter Plug-in für Microsoft Windows installieren und einrichten, wenn Sie Windows-Dateien schützen möchten, bei denen es sich nicht um Datenbankdateien handelt.





## Installationsanforderungen für das SnapCenter -Plug-in für Microsoft Windows

Sie sollten sich bestimmter Installationsanforderungen bewusst sein, bevor Sie das Plug-in für Windows installieren.

Bevor Sie mit der Verwendung des Plug-ins für Windows beginnen, muss der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Sie müssen über SnapCenter Administratorrechte verfügen, um das Plug-in für Windows zu installieren.  
Die SnapCenter Administratorrolle muss über Administratorrechte verfügen.
- Sie müssen den SnapCenter -Server installiert und konfiguriert haben.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie müssen SnapMirror und SnapVault einrichten, wenn Sie eine Backup-Replikation wünschen.

### Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel                                              | Anforderungen                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                      | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> <p>Wenn Sie ein Windows-Cluster-Setup verwenden, sollten Sie auch die Windows-Remoteverwaltung (WinRM) installieren und konfigurieren.</p> |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host | 1 GB                                                                                                                                                                                                                                                                                                    |

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | 5 GB<br><br> 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. |
| Erforderliche Softwarepakete                                                                 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                       |

## Richten Sie Ihre Anmeldeinformationen für das Plug-in für Windows ein

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Windows-Dateisystemen erstellen.

### Was Sie brauchen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.
- Sie müssen die Anmeldeinformationen mit Administratorrechten, einschließlich Administratorrechten, auf dem Remote-Host einrichten.
- Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzer nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzer mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Gehen Sie auf der Seite „Anmeldeinformationen“ wie folgt vor:

| Für dieses Feld...      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Benutzername/Passwort   | <p>Geben Sie den Benutzernamen und das Kennwort ein, die für die Authentifizierung verwendet werden.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> <li>◦ UserName@upn</li> </ul> <ul style="list-style-type: none"> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ lautet wie folgt: UserName</p> <p>Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (&lt;) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als &lt;!10, kleiner als 10 &lt;!, Backtick `12.</p> |
| Passwort                | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ die Anmeldeinformationsverwaltung zuweisen.

## Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

### Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -Effectivelmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$  
.. Fügen Sie der Gruppe Computerobjekte hinzu.  
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des  
Dienstkontos.
```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:
  - a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                |
|---------|----------------|-----------|-----------------------------------------------|
| -----   | -----          | -----     | -----                                         |
| True    | No             | Success   | {Active Directory Domain Services, Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Starten Sie Ihren Host neu.
- b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
- c. Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Hosts hinzufügen und SnapCenter Plug-in für Microsoft Windows installieren

Sie können die SnapCenter -Seite „Host hinzufügen“ verwenden, um Windows-Hosts hinzuzufügen. Das SnapCenter -Plug-in für Microsoft Windows wird automatisch auf dem angegebenen Host installiert. Dies ist die empfohlene Methode zum Installieren von Plug-Ins. Sie können einen Host hinzufügen und ein Plug-In entweder für einen einzelnen Host oder einen Cluster installieren.

### Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Der SnapCenter -Benutzer sollte der Rolle „Als Dienst anmelden“ des Windows-Servers hinzugefügt werden.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

["Konfigurieren Sie das gruppenverwaltete Dienstkonto auf Windows Server 2016 oder höher für das Windows-Dateisystem"](#)

### Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Windows-Plug-Ins
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installieren von Plug-ins auf einem Cluster

Wenn Sie Plug-Ins auf einem Cluster (WSFC, Oracle RAC oder Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert.

- Speicher der E-Serie

Sie können das Plug-in für Windows nicht auf einem Windows-Host installieren, der mit einem Speicher der E-Serie verbunden ist.



SnapCenter unterstützt nicht das Hinzufügen desselben Hosts (Plug-In-Hosts) zu SnapCenter , wenn der Host bereits Teil einer Arbeitsgruppe ist und in eine andere Domäne geändert wurde oder umgekehrt. Wenn Sie denselben Host hinzufügen möchten, sollten Sie den Host aus SnapCenter entfernen und erneut hinzufügen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Gehen Sie auf der Seite „Hosts“ wie folgt vor:

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosttyp              | <p>Wählen Sie den Hosttyp <b>Windows</b> aus.</p> <p>SnapCenter Server fügt den Host hinzu und installiert dann das Plug-in für Windows, falls es nicht bereits auf dem Host installiert ist.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Hostname             | <p>Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.</p> <p>SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den vollqualifizierten Domännennamen (FQDN) einzugeben.</p> <p>Sie können die IP-Adressen oder den FQDN eines der folgenden Elemente eingeben:</p> <ul style="list-style-type: none"> <li>• Eigenständiger Host</li> <li>• Windows Server-Failoverclustering (WSFC)</li> </ul> <p>Wenn Sie mit SnapCenter einen Host hinzufügen und dieser Teil einer Subdomäne ist, müssen Sie den FQDN angeben.</p>                                                                                                                                       |
| Anmeldeinformationen | <p>Wählen Sie den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie die neuen Anmeldeinformationen.</p> <p>Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen einer Anmeldeinformation.</p> <p>Details zu den Anmeldeinformationen, einschließlich Benutzername, Domäne und Hosttyp, werden angezeigt, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div>  <p>Der Authentifizierungsmodus wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

Für neue Bereitstellungen werden keine Plug-In-Pakete aufgelistet.

6. (Optional) Klicken Sie auf **Weitere Optionen**.

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen                                                                                       | <p>Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an.</p> <p>Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |
| Installationspfad                                                                           | <p>Der Standardpfad ist C:\Programme\ NetApp\ SnapCenter.</p> <p>Optional können Sie den Pfad anpassen. Für das SnapCenter Plug-ins-Paket für Windows lautet der Standardpfad C:\Programme\ NetApp\ SnapCenter. Wenn Sie möchten, können Sie den Standardpfad jedoch anpassen.</p>                                                                                                                                                                                                                                                                   |
| Alle Hosts im Cluster hinzufügen                                                            | Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem WSFC hinzuzufügen.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Vorinstallationsprüfungen überspringen                                                      | 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.                                                                                                                                                                                                                                                                                                                                               |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | <p>Aktivieren Sie dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.</p> <p>Geben Sie den gMSA-Namen im folgenden Format an: <i>Domänenname\Kontoname\$</i>.</p> <div>  <p>gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.</p> </div>                                                                                            |

## 7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird überprüft, ob



der Host die Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version und Speicherort werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt.

Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei `web.config` aktualisieren, die sich unter `C:\Program Files\NetApp\SnapCenter WebApp` zum Ändern der Standardwerte. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.



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

8. Überwachen Sie den Installationsfortschritt.

## Installieren Sie das SnapCenter -Plug-in für Microsoft Windows mithilfe von PowerShell-Cmdlets auf mehreren Remotehosts

Wenn Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Hosts gleichzeitig installieren möchten, können Sie dies mithilfe des `Install-SmHostPackage` PowerShell-Cmdlet.

Sie müssen sich auf jedem Host, auf dem Sie Plug-Ins installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung ein, indem Sie `Open-SmConnection` Cmdlet und geben Sie dann Ihre Anmeldeinformationen ein.
3. Fügen Sie den eigenständigen Host oder den Cluster mithilfe des `Add-SmHost` Cmdlet und die erforderlichen Parameter.

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"](#) .

4. Installieren Sie das Plug-in auf mehreren Hosts mithilfe der `Install-SmHostPackage` Cmdlet und die erforderlichen Parameter.

Sie können die `-skipprecheck` Option, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

## Installieren Sie das SnapCenter -Plug-in für Microsoft Windows im Hintergrund über die Befehlszeile

Sie können das SnapCenter -Plug-in für Microsoft Windows lokal auf einem Windows-Host installieren, wenn Sie das Plug-in nicht remote über die SnapCenter -GUI installieren können. Sie können das Installationsprogramm des SnapCenter -Plug-ins für Microsoft Windows unbeaufsichtigt im stillen Modus über die Windows-Befehlszeile ausführen.

## Bevor Sie beginnen

- Sie müssen das Hosting-Paket ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) installiert haben.
- Sie müssen PowerShell 7.4.2 oder höher installiert haben.
- Sie müssen ein lokaler Administrator auf dem Host sein.

## Schritte

1. Laden Sie das SnapCenter -Plug-in für Microsoft Windows von Ihrem Installationsort herunter.

Der Standardinstallationspfad ist beispielsweise C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

2. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-In installieren möchten.
3. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.
4. Geben Sie den folgenden Befehl ein und ersetzen Sie die Variablen durch Ihre Daten:

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""  
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=  
ISFeatureInstall=SCW
```

Beispiel:

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository  
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:  
\HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW`
```



Bei allen während der Installation des Plug-ins für Windows übergebenen Parametern wird zwischen Groß- und Kleinschreibung unterschieden.

Geben Sie die Werte für die folgenden Variablen ein:

| Variable                   | Wert                                                                                                                                                                       |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /debuglog"<Debug_Log_Pfad> | Geben Sie den Namen und den Speicherort der Protokolldatei des Suite-Installationsprogramms an, wie im folgenden Beispiel: Setup.exe /debuglog"C:\PathToLog\setupexe.log". |
| BI_SNAPCENTER_PORT         | Geben Sie den Port an, über den SnapCenter mit SMCORE kommuniziert.                                                                                                        |

| Variable          | Wert                                                                                           |
|-------------------|------------------------------------------------------------------------------------------------|
| SUITE_INSTALLDIR  | Geben Sie das Installationsverzeichnis des Host-Plug-In-Pakets an.                             |
| BI_SERVICEACCOUNT | Geben Sie das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.                  |
| BI_SERVICEPWD     | Geben Sie das Kennwort für das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an. |
| ISFeatureInstall  | Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host bereitgestellt werden soll.    |

Der Parameter *debuglog* enthält den Pfad der Protokolldatei für SnapCenter. Das Schreiben in diese Protokolldatei ist die bevorzugte Methode zum Abrufen von Informationen zur Fehlerbehebung, da die Datei die Ergebnisse der Prüfungen enthält, die die Installation hinsichtlich der Plug-In-Voraussetzungen durchführt.

Bei Bedarf finden Sie zusätzliche Informationen zur Fehlerbehebung in der Protokolldatei für das SnapCenter für Windows-Paket. Die Protokolldateien für das Paket werden (die ältesten zuerst) im Ordner *%Temp%* aufgelistet, beispielsweise *C:\temp\*.



Bei der Installation des Plug-ins für Windows wird das Plug-in auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie können das Plug-In auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder des PowerShell-Cmdlets hinzufügen. Nachdem der Host hinzugefügt wurde, wird das Plug-In automatisch erkannt.

## Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets

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 CA-Zertifikats

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

### CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

#### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige**

## Stammzertifizierungsstellen > Zertifikate.

5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

## Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
  - a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

*Get-ChildItem -Path Zertifikat:\LocalMachine\My*

- b. Kopieren Sie den Fingerabdruck.

### Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

#### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-In-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

### 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.

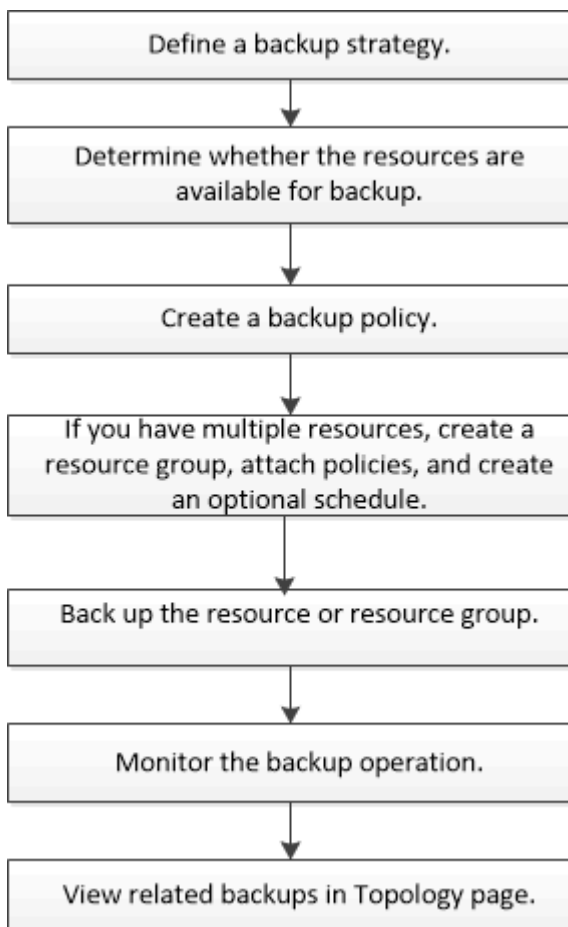
# Sichern Sie Windows-Dateisysteme

## Sichern Sie Windows-Dateisysteme

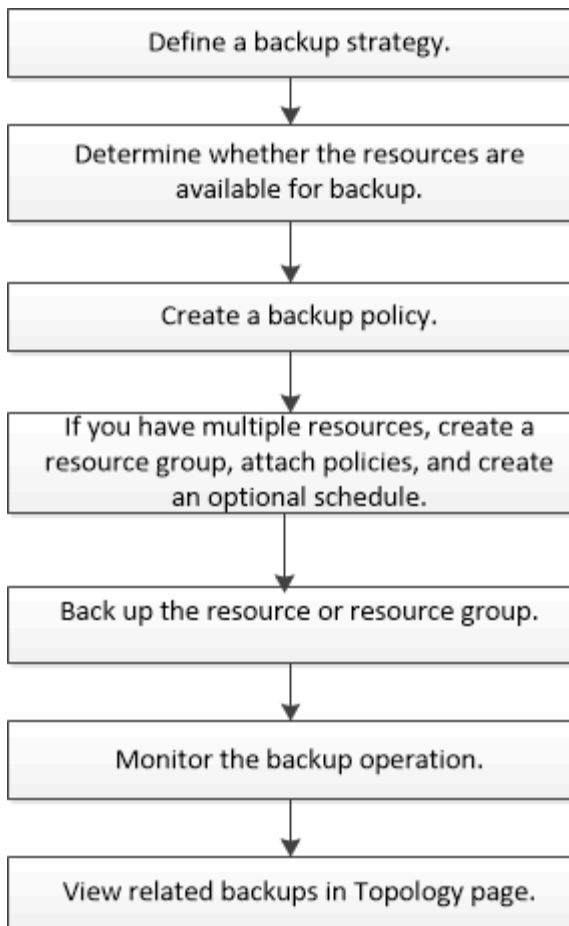
Wenn Sie das SnapCenter -Plug-in für Microsoft Windows in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern von Windows-Dateisystemen verwenden. Sie können ein einzelnes Dateisystem oder eine Ressourcengruppe sichern, die mehrere Dateisysteme enthält. Sie können Backups nach Bedarf oder gemäß einem festgelegten Schutzzeitplan durchführen.

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden. Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Sicherungsvorgänge durchführen müssen:







Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe oder die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) enthält ausführliche Informationen zu PowerShell-Cmdlets.

## Ermitteln der Ressourcenverfügbarkeit für Windows-Dateisysteme

Ressourcen sind die LUNs und ähnliche Komponenten in Ihrem Dateisystem, die von den von Ihnen installierten Plug-Ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datenschutzjobs auf mehreren Ressourcen ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Ihnen zur Verfügung stehen. Durch die Ermittlung verfügbarer Ressourcen wird auch überprüft, ob die Plug-In-Installation erfolgreich abgeschlossen wurde.

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Verbindungen für virtuelle Speichermaschinen (SVM) und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Wenn sich Dateien auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Weitere Informationen finden Sie unter ["SnapCenter Plug-in for VMware vSphere Dokumentation"](#).

### 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“ **Dateisysteme** aus der Liste aus.
3. Wählen Sie den Host aus, um die Liste der Ressourcen zu filtern, und klicken Sie dann auf **Ressourcen aktualisieren**.

Die neu hinzugefügten, umbenannten oder gelöschten Dateisysteme werden im SnapCenter Server-Inventar aktualisiert.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

## Erstellen von Sicherungsrichtlinien für Windows-Dateisysteme

Sie können eine neue Sicherungsrichtlinie für Ressourcen erstellen, bevor Sie SnapCenter zum Sichern von Windows-Dateisystemen verwenden, oder Sie können eine neue Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine Ressource sichern.

### Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben. ["Mehr erfahren"](#)
- Sie müssen sich auf den Datenschutz vorbereitet haben.

Zur Vorbereitung des Datenschutzes müssen Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erkennen von Ressourcen und das Erstellen von Verbindungen zu virtuellen Speichermaschinen (SVM) erledigen.

- 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.
- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des Parameters usePowershellProcessforScripts in der Datei web.config auf true setzen.

Der Standardwert ist „false“

- 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

- Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- 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. Wählen Sie im linken Navigationsbereich **Einstellungen** aus.
2. Wählen Sie auf der Seite „Einstellungen“ **Richtlinien** aus.
3. Wählen Sie **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Sicherung und Replikation“ die folgenden Aufgaben aus:
  - a. Wählen Sie eine Sicherungseinstellung aus.

| Option                                   | Beschreibung                                                                                                                                                                                                                                    |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dateisystemkonsistente Sicherung         | Wählen Sie diese Option, wenn SnapCenter das Festplattenlaufwerk, auf dem sich das Dateisystem befindet, vor Beginn des Sicherungsvorgangs stilllegen und das Festplattenlaufwerk nach Abschluss des Sicherungsvorgangs wieder aktivieren soll. |
| Dateisystem-Absturzkonsistente Sicherung | Wählen Sie diese Option, wenn SnapCenter das Festplattenlaufwerk, auf dem sich das Dateisystem befindet, nicht stilllegen soll.                                                                                                                 |

- b. Wählen Sie eine Zeitplanhäufigkeit (auch Richtlinientyp genannt) aus.

Die Richtlinie gibt nur die Sicherungshäufigkeit an. Der spezifische Schutzzeitplan für die Sicherung wird in der Ressourcengruppe definiert. Daher können zwei oder mehr Ressourcengruppen dieselbe Richtlinie und Sicherungshäufigkeit verwenden, jedoch unterschiedliche Sicherungspläne haben.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- c. Wählen Sie eine Richtlinienbezeichnung aus.

Abhängig von der von Ihnen ausgewählten Snapshot-Bezeichnung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Bezeichnung entspricht.



Wenn Sie \* SnapMirror nach dem Erstellen einer lokalen Snapshot-Kopie aktualisieren\* ausgewählt haben, können Sie optional die sekundäre Richtlinienbezeichnung angeben. Wenn Sie jedoch \* SnapVault nach dem Erstellen einer lokalen Snapshot-Kopie aktualisieren\* ausgewählt haben, sollten Sie die sekundäre Richtlinienbezeichnung angeben.

6. 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 | <p>Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) zu erstellen.</p> <p>Diese Option sollte für die aktive Synchronisierung von SnapSnapMirror aktiviert werden.</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen zugehöriger Sicherungen und Klone auf der Seite „Topologie“"</a> .</p>                                                                                                                                                                                                     |
| Aktualisieren Sie SnapVault nach dem Erstellen einer Snapshot-Kopie                  | <p>Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen.</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche „Aktualisieren“ auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche „Aktualisieren“ auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.</p> <p>Weitere Informationen zu SnapLock Vault finden Sie unter <a href="#">"Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel"</a></p> |

| Für dieses Feld...                     | Machen Sie Folgendes...                                                                                               |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Fehleranzahl der Wiederholungsversuche | Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird. |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

- Geben Sie auf der Seite „Aufbewahrungseinstellungen“ die Aufbewahrungseinstellungen für On-Demand-Backups und für jede von Ihnen ausgewählte Zeitplanhäufigkeit an.

| Option                                          | Beschreibung                                                                                                                                                                          |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gesamtzahl der aufzubewahrenden Snapshot-Kopien | Wählen Sie diese Option, wenn Sie die Anzahl der Snapshots angeben möchten, die SnapCenter speichert, bevor sie automatisch gelöscht werden.                                          |
| Bewahren Sie Snapshot-Kopien für                | Wählen Sie diese Option, wenn Sie die Anzahl der Tage angeben möchten, die SnapCenter eine Sicherungskopie aufbewahrt, bevor sie gelöscht wird.                                       |
| Sperrzeitraum für Snapshot-Kopien               | Wählen Sie den Snapshot-Sperrzeitraum aus und geben Sie die Dauer in Tagen, Monaten oder Jahren an.<br><br>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen. |



Sie sollten die Aufbewahrungsanzahl auf 2 oder höher einstellen. Der Mindestwert für die Aufbewahrungsanzahl beträgt 2.



Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der ONTAP Version unterstützt wird.

- Geben Sie auf der Seite „Skript“ den Pfad des Präskripts oder Postskripts ein, das der SnapCenter -Server vor bzw. nach dem Sicherungsvorgang ausführen soll, sowie ein Zeitlimit, das SnapCenter auf die Ausführung des Skripts wartet, bevor es zu einer Zeitüberschreitung kommt.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren und Protokolle zu senden.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

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

# Erstellen von Ressourcengruppen für Windows-Dateisysteme

Eine Ressourcengruppe ist der Container, zu dem Sie mehrere Dateisysteme hinzufügen können, die Sie schützen möchten. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzauftrags zu definieren, den Sie ausführen möchten, und dann den Sicherungszeitplan angeben.

## Informationen zu diesem Vorgang

- 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.
- 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. 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“ **Dateisysteme** aus der Liste aus.



Wenn Sie SnapCenter kürzlich ein Dateisystem hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie auf **Neue Ressourcengruppe**.
4. Führen Sie auf der Seite „Name“ des Assistenten die folgenden Schritte aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | Geben Sie den Namen der Ressourcengruppe ein. <div><div></div><div>Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</div></div>                                                                                                          |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein.<br><br>Beispiel:<br>customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt. |
| Etikett                                                       | Geben Sie ein beschreibendes Tag ein, um die Suche nach einer Ressourcengruppe zu erleichtern.                                                                                                                                                                  |

5. Führen Sie auf der Seite „Ressourcen“ die folgenden Aufgaben aus:

- a. Wählen Sie den Host aus, um die Liste der Ressourcen zu filtern.

Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

- b. Klicken Sie im Abschnitt „Verfügbare Ressourcen“ auf die Dateisysteme, die Sie sichern möchten, und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt „Hinzugefügt“ zu verschieben.

Wenn Sie die Option **Alle Ressourcen auf demselben Speichervolume automatisch auswählen** auswählen, werden alle Ressourcen auf demselben Volume ausgewählt. Wenn Sie sie in den Abschnitt „Hinzugefügt“ verschieben, werden alle Ressourcen auf diesem Volume zusammen verschoben.

Um ein einzelnes Dateisystem hinzuzufügen, deaktivieren Sie die Option **Alle Ressourcen auf demselben Speichervolume automatisch auswählen** und wählen Sie dann die Dateisysteme aus, die Sie in den Abschnitt „Hinzugefügt“ verschieben möchten.

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Aufgaben aus:

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

Sie können eine beliebige vorhandene Richtlinie auswählen und auf **Details** klicken, um festzustellen, ob Sie diese Richtlinie verwenden können.

Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine neue Richtlinie erstellen, indem Sie auf \* klicken.  \* um den Richtlinienassistenten zu starten.

Die ausgewählten Richtlinien werden in der Spalte „Richtlinie“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

- b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
- c. Wenn die Richtlinie mit mehreren Zeitplantypen (Häufigkeiten) verknüpft ist, wählen Sie die Häufigkeit aus, die Sie konfigurieren möchten.
- d. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **Fertig**.

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden. Sie sollten die Zeitpläne des Windows-Taskplaners und des SQL Server-Agenten nicht ändern.

7. Geben Sie auf der Seite „Benachrichtigung“ die folgenden Benachrichtigungsinformationen ein:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-Mail-Präferenz   | Wählen Sie <b>Immer</b> , <b>Bei Fehler</b> oder <b>Bei Fehler oder Warnung</b> aus, um nach dem Erstellen von Sicherungsressourcengruppen, dem Anhängen von Richtlinien und dem Konfigurieren von Zeitplänen E-Mails an Empfänger zu senden. Geben Sie den SMTP-Server, die Standard-E-Mail-Betreffzeile sowie die E-Mail-Adressen „An“ und „Von“ ein. |
| Aus                | E-Mail-Adresse                                                                                                                                                                                                                                                                                                                                          |
| Zu                 | E-Mail an Adresse                                                                                                                                                                                                                                                                                                                                       |
| Betreff            | Standardmäßige E-Mail-Betreffzeile                                                                                                                                                                                                                                                                                                                      |

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

Sie können eine Sicherung bei Bedarf durchführen oder auf die geplante Sicherung warten.

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Windows-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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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 <b>Überprüfung nach Sicherung ausführen</b> .                                                        |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Ausführen von Datenschutzvorgängen verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Verwaltungs-LIF-IP-Adresse haben.

### Schritte

- Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets `Open-SmConnection`.

Dieses Beispiel öffnet eine PowerShell-Sitzung:

```
PS C:\> Open-SmConnection
```

- Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

- Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

In diesem Beispiel wird eine neue Anmeldeinformation mit dem Namen „FinanceAdmin“ mit Windows-Anmeldeinformationen erstellt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

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"](#).

## Sichern Sie bei Bedarf eine einzelne Ressource für Windows-Dateisysteme

Wenn sich eine Ressource nicht in einer Ressourcengruppe befindet, können Sie die Ressource bei Bedarf auf der Seite „Ressourcen“ sichern.

### Informationen zu diesem Vorgang

Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.



Beim Sichern eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount Point (VMP) im zu sichernden Dateisystem gemountet sind.



Wenn Sie im Kontext eines Windows-Dateisystems arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht eine inkonsistente Sicherung und es kann beim Wiederherstellen zu Datenverlust kommen. Zum Schutz von Datenbankdateien müssen Sie das entsprechende SnapCenter -Plug-in für die Datenbank verwenden (z. B. SnapCenter -Plug-in für Microsoft SQL Server oder SnapCenter -Plug-in für Microsoft Exchange Server).

## SnapCenter -Benutzeroberfläche

### 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“ den Ressourcentyp „Dateisystem“ und dann die Ressource aus, die Sie sichern möchten.
3. Wenn der Assistent „Dateisystem – Schützen“ nicht automatisch startet, klicken Sie auf **Schützen**, um den Assistenten zu starten.

Geben Sie die Schutzeinstellungen an, wie in den Aufgaben zum Erstellen von Ressourcengruppen beschrieben.

4. Optional: Geben Sie auf der Ressourcenseite des Assistenten ein benutzerdefiniertes Namensformat für den Snapshot ein.

Beispiel: customtext\_resourcegroup\_policy\_hostname oder resourcegroup\_hostname.  
Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Richtlinien“ die folgenden Aufgaben aus:

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

Sie können eine beliebige vorhandene Richtlinie auswählen und dann auf **Details** klicken, um festzustellen, ob Sie diese Richtlinie verwenden können.

Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine vorhandene Richtlinie kopieren und ändern oder eine neue Richtlinie erstellen, indem Sie auf  , um den Richtlinienassistenten zu starten. Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine vorhandene Richtlinie kopieren und ändern oder eine neue Richtlinie erstellen, indem Sie auf  , um den Richtlinienassistenten zu starten.

Die ausgewählten Richtlinien werden in der Spalte „Richtlinie“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

- b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf  in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **Fertig**.

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

**"Geplante Vorgänge können fehlschlagen"**

6. Führen Sie auf der Seite „Benachrichtigung“ die folgenden Aufgaben aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-Mail-Präferenz   | Wählen Sie <b>Immer</b> , <b>Bei Fehler</b> oder <b>Bei Fehler oder Warnung</b> aus, um nach dem Erstellen von Sicherungsressourcengruppen, dem Anhängen von Richtlinien und dem Konfigurieren von Zeitplänen E-Mails an Empfänger zu senden.<br><br>Geben Sie die SMTP-Serverinformationen, die Standard-Betreffzeile der E-Mail sowie die E-Mail-Adressen „An“ und „Von“ ein. |
| Aus                | E-Mail-Adresse                                                                                                                                                                                                                                                                                                                                                                  |
| Zu                 | E-Mail an Adresse                                                                                                                                                                                                                                                                                                                                                               |
| Betreff            | Standardmäßige E-Mail-Betreffzeile                                                                                                                                                                                                                                                                                                                                              |

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

Die Seite „Datenbanktopologie“ wird angezeigt.

8. Klicken Sie auf **Jetzt sichern**.

9. 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**.

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

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem SQL-Sicherungstyp „FullBackup“ erstellt:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy  
-PluginPolicyType SCSQL -PolicyType Backup  
-SqlBackupType FullBackup -Verbose
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem Sicherungstyp „CrashConsistent“ für das Windows-Dateisystem erstellt:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy  
-PluginPolicyType SCW -PolicyType Backup  
-ScwBackupType CrashConsistent -Verbose
```

### 3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „Get-SmResources“.

Dieses Beispiel ermittelt die Ressourcen für das Microsoft SQL-Plug-In auf dem angegebenen Host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCSQL
```

Dieses Beispiel ermittelt die Ressourcen für Windows-Dateisysteme auf dem angegebenen Host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com  
-PluginCode SCW
```

### 4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

In diesem Beispiel wird eine neue SQL-Datenbank-Sicherungsressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource  
-Resources @{"Host"="visef6.org.com";  
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}  
-Policies "BackupPolicy"
```

In diesem Beispiel wird eine neue Ressourcengruppe zur Sicherung des Windows-Dateisystems mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource  
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";  
"Type"="Windows Filesystem";"Names"="E:\"}  
-Policies "EngineeringBackupPolicy"
```

5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

In diesem Beispiel wird ein Job-Zusammenfassungsbericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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"](#) .

## Sichern von Ressourcengruppen für Windows-Dateisysteme

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt. Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror -Beziehung zum sekundären Speicher sichern möchten, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet ausgelöst wird. Sie sollten den Wert von MaxRetryForUninitializedHosts in web.config mithilfe des PowerShell-Cmdlets Set-SmConfigSettings konfigurieren.



Beim Sichern eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount Point (VMP) im zu sichernden Dateisystem gemountet sind.



Wenn Sie im Kontext eines Windows-Dateisystems arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht eine inkonsistente Sicherung und es kann beim Wiederherstellen zu Datenverlust kommen. Zum Schutz von Datenbankdateien müssen Sie das entsprechende SnapCenter -Plug-in für die Datenbank verwenden (z. B. SnapCenter -Plug-in für Microsoft SQL Server oder SnapCenter -Plug-in für Microsoft Exchange Server).

### 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 „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf  und wählen Sie das Tag aus. Sie können dann auf , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.



Wenn Sie beim SnapCenter Plug-in für Oracle Database über eine föderierte Ressourcengruppe mit zwei Datenbanken verfügen und eine der Datenbanken eine Datendatei auf einem Nicht- NetApp -Speicher hat, wird der Sicherungsvorgang abgebrochen, obwohl sich die andere Datenbank auf einem NetApp -Speicher befindet.

4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
  - a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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**.

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

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

**"SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"**

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl. Um die Größe des Java-Heaps zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`.

## Überwachen von Sicherungsvorgängen

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 Vorgängen 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.

## Abbrechen von Sicherungsvorgängen

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li><li>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                          |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>b. Wählen Sie den Vorgang aus.</li><li>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li></ol> |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## Anzeigen zugehöriger Sicherungen und Klone auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, können Sie eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzeigen. Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um

## Datenschutzvorgänge durchzuführen.

### Informationen zu diesem Vorgang

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.
-  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.
-  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. Nur für Oracle-Datenbanken wird im Abschnitt „Zusammenfassungskarte“ auch die Gesamtzahl der Protokollsicherungen 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 die Anwendungsressource auf 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-, Umbenennungs- und Löschvorgänge durchzuführen.

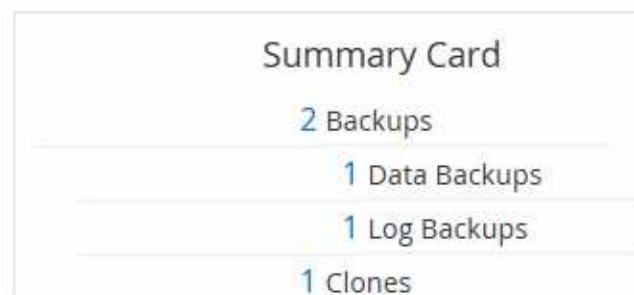
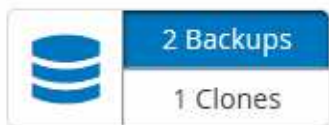


Sie können Sicherungen, die sich auf dem sekundären Speichersystem befinden, weder umbenennen noch löschen.

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

### Beispiel für Backups und Klone auf dem Primärspeicher

## Manage Copies



## Bereinigen der Anzahl sekundärer Sicherungen mithilfe von PowerShell-Cmdlets

Sie können das Cmdlet „Remove-SmBackup“ verwenden, um die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshot zu bereinigen. Sie können dieses Cmdlet verwenden, wenn die Gesamtzahl der in der Topologie „Kopien verwalten“ angezeigten Snapshots nicht mit der Snapshot-Aufbewahrungseinstellung des sekundären Speichers übereinstimmt.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

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. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Bereinigen Sie die Anzahl sekundärer Sicherungen mit dem Parameter -CleanupSecondaryBackups.

In diesem Beispiel wird die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshots bereinigt:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s) .
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

## Wiederherstellen von Windows-Dateisystemen

### Wiederherstellen von Windows-Dateisystemsicherungen

Sie können SnapCenter verwenden, um Dateisystemsicherungen wiederherzustellen. Die

Wiederherstellung des Dateisystems ist ein mehrphasiger Prozess, bei dem alle Daten aus einer angegebenen Sicherung an den ursprünglichen Speicherort des Dateisystems kopiert werden.

#### **Bevor Sie beginnen**

- Sie müssen das Dateisystem gesichert haben.
- Wenn für ein Dateisystem gerade ein geplanter Vorgang ausgeführt wird, beispielsweise ein Sicherungsvorgang, muss dieser Vorgang abgebrochen werden, bevor Sie einen Wiederherstellungsvorgang starten können.
- Sie können eine Dateisystemsicherung nur am ursprünglichen Speicherort wiederherstellen, nicht auf einem alternativen Pfad.

Sie können aus einer Sicherung keine einzelne Datei wiederherstellen, da das wiederhergestellte Dateisystem alle Daten am ursprünglichen Speicherort des Dateisystems überschreibt. Um eine einzelne Datei aus einer Dateisystemsicherung wiederherzustellen, müssen Sie die Sicherung klonen und auf die Datei im Klon zugreifen.

- Sie können ein System- oder Startvolume nicht wiederherstellen.
- SnapCenter kann Dateisysteme in einem Windows-Cluster wiederherstellen, ohne die Clustergruppe offline zu nehmen.

#### **Informationen zu diesem Vorgang**

- Der `SCRIPTS_PATH` wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: `API /4.7/configsettings`

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

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

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Um die Liste der Ressourcen zu filtern, wählen Sie die Optionen „Dateisystem“ und „Ressourcengruppe“ aus.
3. Wählen Sie eine Ressourcengruppe aus der Liste aus und klicken Sie dann auf **Wiederherstellen**.
4. Wählen Sie auf der Seite „Sicherungen“ aus, ob Sie von primären oder sekundären Speichersystemen wiederherstellen möchten, und wählen Sie dann eine wiederherzustellende Sicherung aus.
5. Wählen Sie Ihre Optionen im Wiederherstellungsassistenten aus.
6. Sie können den Pfad und die Argumente des Präskripts oder Postskripts eingeben, das SnapCenter vor bzw. nach dem Wiederherstellungsvorgang ausführen soll.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

7. Wählen Sie auf der Benachrichtigungsseite eine der folgenden Optionen aus:

| Für dieses Feld...                                                                               | Machen Sie Folgendes...                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protokollieren Sie SnapCenter Serverereignisse im Syslog des Speichersystems                     | Wählen Sie diese Option, um SnapCenter Server-Ereignisse im Syslog des Speichersystems zu protokollieren.                                                                                                                                                                                       |
| Senden Sie eine AutoSupport -Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem | Wählen Sie diese Option, um Informationen zu fehlgeschlagenen Vorgängen mithilfe von AutoSupport an NetApp zu senden.                                                                                                                                                                           |
| E-Mail-Präferenz                                                                                 | Wählen Sie <b>Immer</b> , <b>Bei Fehler</b> oder <b>Bei Fehler oder Warnung</b> aus, um nach der Wiederherstellung von Sicherungen E-Mail-Nachrichten an die Empfänger zu senden. Geben Sie den SMTP-Server, die Standard-Betreffzeile der E-Mail sowie die E-Mail-Adressen „An“ und „Von“ ein. |

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
9. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.





Wenn das wiederhergestellte Dateisystem eine Datenbank enthält, müssen Sie auch die Datenbank wiederherstellen. Wenn Sie die Datenbank nicht wiederherstellen, befindet sich Ihre Datenbank möglicherweise in einem ungültigen Zustand. Informationen zum Wiederherstellen von Datenbanken finden Sie im Datenschutzhandbuch für die jeweilige Datenbank.

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „`Get-SmBackup`“ und „`Get-SmBackupReport`“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime           | BackupType  |
|----------|-------------------------------|----------------------|-------------|
| -----    | -----                         | -----                | -----       |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:02:32 AM | Full Backup |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:23:17 AM |             |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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"](#) .

## Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets

Das Wiederherstellen einer Ressourcensicherung umfasst das Einleiten einer Verbindungssitzung mit dem SnapCenter -Server, das Auflisten der Sicherungen und Abrufen von Sicherungsinformationen sowie das Wiederherstellen einer Sicherung.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId    | BackupName                    | BackupTime           |
|-------------|-------------------------------|----------------------|
| BackupType  |                               |                      |
| -----       | -----                         | -----                |
| 1           | Payroll Dataset_vise-f6_08... | 8/4/2015 11:02:32 AM |
| Full Backup |                               |                      |
| 2           | Payroll Dataset_vise-f6_08... | 8/4/2015 11:23:17 AM |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDateTime "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :

```

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"](#).

## Überwachen von Wiederherstellungsvorgängen

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.

## Abbrechen von Wiederherstellungsvorgängen

Sie können in der Warteschlange befindliche Wiederherstellungsaufträge abbrechen.

Sie sollten als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzuberechnen.

### Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Wiederherstellungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Wiederherstellungsvorgänge abzuberechnen.
- Die Schaltfläche **Auftrag abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li><li>2. Wählen Sie den Auftrag aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                                     |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>2. Wählen Sie den Vorgang aus.</li><li>3. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li></ol> |

## Klonen Sie Windows-Dateisysteme

### Klonen aus einer Windows-Dateisystemsicherung

Sie können SnapCenter verwenden, um eine Windows-Dateisystemsicherung zu klonen. Wenn Sie eine Kopie einer einzelnen Datei wünschen, die versehentlich gelöscht oder geändert wurde, können Sie eine Sicherungskopie klonen und im Klon auf diese Datei zugreifen.

#### Bevor Sie beginnen

- Sie sollten sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Verbindungen zu virtuellen Speichermaschinen (SVM) erledigt haben.
- Sie sollten über eine Sicherungskopie des Dateisystems verfügen.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Sie können eine Ressourcengruppe nicht klonen. Sie können nur einzelne Dateisystemsicherungen klonen.
- Wenn sich eine Sicherung auf einer virtuellen Maschine mit einer VMDK-Festplatte befindet, kann SnapCenter die Sicherung nicht auf einen physischen Server klonen.
- Wenn Sie einen Windows-Cluster klonen (z. B. eine freigegebene LUN oder eine Cluster Shared Volume (CSV)-LUN), wird der Klon als dedizierte LUN auf dem von Ihnen angegebenen Host gespeichert.
- Bei einem Klonvorgang darf das Stammverzeichnis des Volume-Mount-Punkts kein freigegebenes Verzeichnis sein.
- Sie können keinen Klon auf einem Knoten erstellen, der nicht der Home-Knoten für das Aggregat ist.
- Sie können für Windows-Dateisysteme keine wiederkehrenden Klonvorgänge (Klon-Lebenszyklus) planen. Sie können eine Sicherung nur bei Bedarf klonen.
- Wenn Sie eine LUN, die einen Klon enthält, auf ein neues Volume verschieben, kann SnapCenter den Klon nicht mehr unterstützen. Beispielsweise können Sie SnapCenter nicht zum Löschen dieses Klons



verwenden.

- Sie können nicht über Umgebungen hinweg klonen. Beispielsweise das Klonen von einer physischen Festplatte auf eine virtuelle Festplatte oder umgekehrt.

#### **Informationen zu diesem Vorgang**

- Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- 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.

## SnapCenter -Benutzeroberfläche

### 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“ **Dateisysteme** aus der Liste aus.
3. Wählen Sie den Host aus.

Die Topologieansicht wird automatisch angezeigt, wenn die Ressource geschützt ist.

4. Wählen Sie aus der Ressourcenliste das Backup aus, das Sie klonen möchten, und klicken Sie dann auf das Klonensymbol.
5. Gehen Sie auf der Seite „Optionen“ wie folgt vor:

| Für dieses Feld...                                                                         | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server klonen                                                                              | Wählen Sie den Host aus, auf dem der Klon erstellt werden soll.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| „Mountpunkt automatisch zuweisen“ oder „Volume-Mountpunkt automatisch unter Pfad zuweisen“ | <p>Wählen Sie, ob automatisch ein Bereitstellungspunkt oder ein Volume-Bereitstellungspunkt unter einem Pfad zugewiesen werden soll.</p> <p>Automatische Zuweisung des Volume-Mount-Punkts unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht Ihnen, ein bestimmtes Verzeichnis anzugeben, in dem die Mount-Punkte erstellt werden. Bevor Sie diese Option wählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich im Verzeichnis eine Sicherung befindet, befindet sich die Sicherung nach dem Mount-Vorgang in einem ungültigen Zustand.</p> |
| Archivspeicherort                                                                          | Wählen Sie einen Archivspeicherort, wenn Sie eine sekundäre Sicherung klonen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

6. Geben Sie auf der Skriptseite alle Präskripte oder Postskripte an, die Sie ausführen möchten.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
8. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

### PowerShell-Cmdlets

#### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Sicherungen auf, die mit dem Cmdlet Get-SmBackup oder Get-SmResourceGroup geklont werden können.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
C:\PS>PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime              | BackupType  |
|----------|-------------------------------|-------------------------|-------------|
| -----    | -----                         | -----                   | -----       |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015<br>11:02:32 AM | Full Backup |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015<br>11:23:17 AM |             |

In diesem Beispiel werden Informationen zu einer angegebenen Ressourcengruppe, ihren Ressourcen und zugehörigen Richtlinien angezeigt:

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
```

SearchResources : False  
ByPassCredential : False  
IsCustomSnapshot :  
MaintenanceStatus : Production  
PluginProtectionGroupTypes : {SMSQL}  
Name : Payrolldataset  
Type : Group  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
ApplySnapvaultUpdate : False  
ApplyRetention : False  
RetentionCount : 0  
RetentionDays : 0  
ApplySnapMirrorUpdate : False  
SnapVaultLabel :  
MirrorVaultUpdateRetryCount : 7  
AppPolicies : {}  
Description : FinancePolicy  
PreScriptPath :  
PreScriptArguments :  
PostScriptPath :  
PostScriptArguments :  
ScriptTimeout : 60000  
DateModified : 8/4/2015 3:43:30 PM  
DateCreated : 8/4/2015 3:43:30 PM  
Schedule : SMCoreContracts.SmSchedule  
PolicyType : Backup  
PluginPolicyType : SMSQL  
Name : FinancePolicy  
Type :  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
clab-a13-13.sddev.lab.netapp.com  
DatabaseGUID :

```

SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. Starten Sie einen Klonvorgang aus einer vorhandenen Sicherung mithilfe des Cmdlets New-SmClone.

Dieses Beispiel erstellt einen Klon aus einem angegebenen Backup mit allen Protokollen:

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

In diesem Beispiel wird ein Klon einer angegebenen Microsoft SQL Server-Instanz erstellt:

```
PS C:\> New-SmClone
-B BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-R Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-A AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-S Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

#### 4. Zeigen Sie den Status des Klonauftrags mithilfe des Cmdlets Get-SmCloneReport an.

Dieses Beispiel zeigt einen Klonbericht für die angegebene Job-ID an:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

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"](#) .

## Überwachen von Klonvorgängen

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**.

## Abbrechen von Klonvorgängen

Sie können in der Warteschlange befindliche Klonvorgänge abbrechen.

Sie sollten als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Klonvorgänge abzuberechnen.

### Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Klonvorgang entweder auf der Seite **Monitor** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Klonvorgänge abzuberechnen.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"> <li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li> <li>2. Wählen Sie den Vorgang aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li> </ol>                                                                                                                                                                           |
| Aktivitätsbereich | <ol style="list-style-type: none"> <li>1. Klicken Sie nach dem Starten des Klonvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li> <li>2. Wählen Sie den Vorgang aus.</li> <li>3. Klicken Sie auf der Seite <b>Auftragsdetails</b> auf <b>Auftrag abbrechen</b>.</li> </ol> |

## 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 <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme         | Wählen Sie <b>Pfad</b> 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"](#)

# Schützen Sie Microsoft Exchange Server-Datenbanken

## SnapCenter Plug-in für Microsoft Exchange Server-Konzepte

### Übersicht über das SnapCenter -Plug-in für Microsoft Exchange Server

Das SnapCenter -Plug-in für Microsoft Exchange Server ist eine hostseitige Komponente der NetApp SnapCenter -Software, die eine anwendungsbewusste Datenschutzverwaltung von Exchange-Datenbanken ermöglicht. Das Plug-in für Exchange automatisiert die Sicherung und Wiederherstellung von Exchange-Datenbanken in Ihrer SnapCenter -Umgebung.

Wenn das Plug-in für Exchange installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und mit der NetApp SnapVault -Technologie eine Disk-to-Disk-Sicherungsreplikation zur Einhaltung von Standards oder zu Archivierungszwecken durchführen.

Wenn Sie statt der gesamten Exchange-Datenbank E-Mails oder Postfächer wiederherstellen möchten, können Sie die Software Single Mailbox Recovery (SMBR) verwenden. Die Verfügbarkeit von NetApp® Single Mailbox Recovery (EOA) endet am 12. Mai 2023. NetApp wird Kunden, die Postfachkapazität, Wartung und Support über die am 24. Juni 2020 eingeführten Marketing-Teilenummern erworben haben, für die Dauer des Supportanspruchs weiterhin unterstützen.

NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. Ontrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können neue Ontrack PowerControls-Softwarelizenzen sowie Wartungs- und Supportverlängerungen für Ontrack PowerControls von Ontrack (über [licensingteam@ontrack.com](mailto:licensingteam@ontrack.com)) für eine detaillierte Postfachwiederherstellung erwerben.

Das Plug-in für Exchange unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie ein transparentes Failover durchführen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

Es unterstützt den asymmetrischen, Failover- oder Nicht-Duplex-Modus von SnapMirror Active Sync. Dies bezieht sich auf die Lösung, bei der der optimierte Pfad nur vom primärseitigen LUN-Eigentümerknoten ausgeht. Alle E/A-Vorgänge auf den sekundären Clusterpfaden werden durch Proxy-Weiterleitung an den primären Cluster abgewickelt. Die synchrone Replikation erfolgt unidirektional, vom Primär- zum Sekundärserver.

- Automatisiert anwendungsorientierte Sicherungs- und Wiederherstellungsvorgänge für Microsoft Exchange Server-Datenbanken und Database Availability Groups (DAGs) in Ihrer SnapCenter Umgebung
- Unterstützt virtualisierte Exchange-Server auf RDM-LUNs, wenn Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.

## Was Sie mit dem SnapCenter Plug-in für Microsoft Exchange Server tun können

Sie können das Plug-in für Exchange zum Sichern und Wiederherstellen von Exchange Server-Datenbanken verwenden.

- Anzeigen und Verwalten eines aktiven Inventars von Exchange Database Availability Groups (DAGs), Datenbanken und Replikatsätzen
- Definieren Sie Richtlinien, die die Schutzeinstellungen für die Backup-Automatisierung bereitstellen
- Zuweisen von Richtlinien zu Ressourcengruppen
- Schützen Sie einzelne DAGs und Datenbanken
- Sichern Sie primäre und sekundäre Exchange-Postfachdatenbanken
- Wiederherstellen von Datenbanken aus primären und sekundären Sicherungen

## Vom SnapCenter Plug-in für Microsoft Windows und Microsoft Exchange Server unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen als auch auf virtuellen Maschinen. Sie müssen überprüfen, ob für Ihren Speichertyp Unterstützung verfügbar ist, bevor Sie das Paket für Ihren Host installieren.

SnapCenter -Bereitstellungs- und Datenschutzunterstützung ist auf Windows Server verfügbar. Die neuesten Informationen zu unterstützten Versionen finden Sie im <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT> [NetApp Interoperabilitätsmatrix-Tool^].

| Maschine          | Speichertyp                                                                  | Bereitstellung mittels                                                    | Support-Hinweise                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | FC-verbundene LUNs                                                           | Grafische Benutzeroberfläche (GUI) von SnapCenter oder PowerShell-Cmdlets |                                                                                                                                                               |
| Physischer Server | Über iSCSI verbundene LUNs                                                   | SnapCenter -GUI oder PowerShell-Cmdlets                                   |                                                                                                                                                               |
| VMware VM         | Über einen FC- oder iSCSI-HBA verbundene RDM-LUNs                            | PowerShell-Cmdlets                                                        | Nur physikalische Kompatibilität<br><br> VMDKs werden nicht unterstützt. |
| VMware VM         | iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind | SnapCenter -GUI oder PowerShell-Cmdlets                                   |  VMDKs werden nicht unterstützt.                                         |

| Maschine   | Speichertyp                                                                             | Bereitstellung mittels                  | Support-Hinweise                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hyper-V-VM | Virtuelle FC (vFC) LUNs, die durch einen virtuellen Fibre Channel Switch verbunden sind | SnapCenter -GUI oder PowerShell-Cmdlets | <p>Sie müssen Hyper-V Manager verwenden, um Virtual FC (vFC)-LUNs bereitzustellen, die über einen virtuellen Fibre Channel-Switch verbunden sind.</p> <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div> |
| Hyper-V-VM | iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind            | SnapCenter -GUI oder PowerShell-Cmdlets | <div>  <p>Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp-Speicher bereitgestellt werden, werden nicht unterstützt.</p> </div>                                                                                                                                                     |

## Für das Exchange-Plug-In sind mindestens ONTAP Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN erstellen
  - LUN erstellen
  - LUN löschen
  - lun igroup hinzufügen
  - lun igroup erstellen
  - LUN-Igroup löschen
  - LUN-Igroup umbenennen
  - LUN-Igroup umbenennen
  - lun igroup show
  - LUN-Zuordnung Add-Reporting-Nodes
  - LUN-Zuordnung erstellen
  - LUN-Zuordnung löschen
  - LUN-Zuordnung zum Entfernen von Berichtsknoten
  - LUN-Mapping-Show
  - LUN ändern
  - LUN-Einzugsvolumen
  - lun offline
  - lun online
  - LUN persistent-reservation clear
  - LUN-Größe ändern
  - LUN-Seriennummer
  - Lun-Show
  - Snapmirror-Richtlinie Add-Rule
  - Snapmirror-Richtlinienänderungsregel
  - Snapmirror-Richtlinie zum Entfernen der Regel
  - Snapmirror-Richtlinien-Show
  - Snapmirror-Wiederherstellung
  - Snapmirror-Show
  - Snapmirror-Showverlauf
  - Snapmirror-Update
  - Snapmirror-Update-LS-Set

- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen

- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle anzeigen
  - vServer

## Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#).

## Definieren Sie eine Sicherungsstrategie für Exchange Server-Ressourcen

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge können Sie sicherstellen, dass Sie über die Sicherungen verfügen, die Sie für eine erfolgreiche Wiederherstellung Ihrer Datenbanken benötigen. Ihre Sicherungsstrategie wird weitgehend von Ihrem Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmt.

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Die RTO ist die Zeit, bis zu der ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt sein muss. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Backup-Strategie bei.

### Für die Exchange-Datenbank unterstützte Sicherungstypen

Zum Sichern von Exchange-Postfächern mit SnapCenter müssen Sie den Ressourcentyp auswählen, z. B. Datenbanken und Database Availability Groups (DAG). Mithilfe der Snapshot-Technologie werden schreibgeschützte Onlinekopien der Volumes erstellt, auf denen sich die Ressourcen befinden.

| Sicherungstyp                                 | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vollständige Sicherung und Protokollsicherung | <p>Sichert die Datenbanken und alle Transaktionsprotokolle, einschließlich der gekürzten Protokolle.</p> <p>Nach Abschluss einer vollständigen Sicherung kürzt der Exchange Server die Transaktionsprotokolle, die bereits in der Datenbank gespeichert sind.</p> <p>Normalerweise sollten Sie diese Option wählen. Wenn Ihre Sicherungszeit jedoch kurz ist, können Sie bei einer vollständigen Sicherung auf die Ausführung einer Transaktionsprotokollsicherung verzichten.</p> |
| Vollständige Sicherung                        | <p>Sichert Datenbanken und Transaktionsprotokolle.</p> <p>Die gekürzten Transaktionsprotokolle werden nicht gesichert.</p>                                                                                                                                                                                                                                                                                                                                                         |
| Protokollsicherung                            | <p>Sichert alle Transaktionsprotokolle.</p> <p>Die gekürzten Protokolle, die bereits in der Datenbank gespeichert sind, werden nicht gesichert. Wenn Sie zwischen vollständigen Datenbanksicherungen häufige Transaktionsprotokollsicherungen planen, können Sie granulare Wiederherstellungspunkte auswählen.</p>                                                                                                                                                                 |

### Sicherungszeitpläne für Datenbank-Plugins

Die Sicherungshäufigkeit (Zeitplantyp) wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler



wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen. Beispielsweise können regelmäßige Sicherungen des Transaktionsprotokolls ausreichen, um sicherzustellen, dass Sie über die erforderlichen Sicherungen verfügen. Je häufiger Sie Ihre Datenbanken sichern, desto weniger Transaktionsprotokolle muss SnapCenter zum Zeitpunkt der Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können als Sicherungshäufigkeit für die Richtlinie stündlich, täglich, wöchentlich oder monatlich auswählen. Wenn Sie keine dieser Frequenzen auswählen, handelt es sich bei der erstellten Richtlinie um eine Nur-On-Demand-Richtlinie. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen > Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen > Ressourcengruppen** klicken.

## Anzahl der für Datenbanken benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

## Namenskonventionen für Backups

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: customtext\_resourcegroup\_policy\_hostname oder resourcegroup\_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

### Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.



Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

### Wie lange sollen Transaktionsprotokollsicherungen auf dem Quellspeichervolume für Exchange Server aufbewahrt werden?

Das SnapCenter Plug-in für Microsoft Exchange Server benötigt Transaktionsprotokollsicherungen, um aktuelle Wiederherstellungsvorgänge durchzuführen, die Ihre Datenbank auf einen Zeitpunkt zwischen zwei vollständigen Sicherungen wiederherstellen.

Wenn Plug-in for Exchange beispielsweise um 8:00 Uhr eine vollständige Sicherung plus Transaktionsprotokoll und um 17:00 Uhr eine weitere vollständige Sicherung plus Transaktionsprotokoll erstellt hat, kann es die neueste Transaktionsprotokollsicherung verwenden, um die Datenbank auf einen beliebigen Zeitpunkt zwischen 8:00 und 17:00 Uhr wiederherzustellen. Wenn keine Transaktionsprotokolle verfügbar sind, kann Plug-in for Exchange nur zeitpunktbezogene Wiederherstellungsvorgänge durchführen, die eine Datenbank auf den Zeitpunkt wiederherstellen, zu dem Plug-in for Exchange eine vollständige Sicherung abgeschlossen hat.

Normalerweise benötigen Sie aktuelle Wiederherstellungsvorgänge nur für ein oder zwei Tage. Standardmäßig behält SnapCenter mindestens zwei Tage.

### Definieren einer Wiederherstellungsstrategie für Exchange-Datenbanken

Durch die Definition einer Wiederherstellungsstrategie für Exchange Server können Sie Ihre Datenbank erfolgreich wiederherstellen.

#### Quellen für einen Wiederherstellungsvorgang in Exchange Server

Sie können eine Exchange Server-Datenbank aus einer Sicherungskopie auf dem primären Speicher wiederherstellen.

Sie können Datenbanken nur aus dem Primärspeicher wiederherstellen.

## Für Exchange Server unterstützte Arten von Wiederherstellungsvorgängen

Sie können SnapCenter verwenden, um verschiedene Arten von Wiederherstellungsvorgängen an Exchange-Ressourcen durchzuführen.

- Aktuelle Wiederherstellung
- Wiederherstellen eines früheren Zeitpunkts

### Wiederherstellung auf die Minute genau

Bei einem minutengenauen Wiederherstellungsvorgang werden Datenbanken bis zum Fehlerpunkt wiederhergestellt. SnapCenter erreicht dies durch Ausführen der folgenden Sequenz:

1. Stellt die Datenbanken aus der von Ihnen ausgewählten vollständigen Datenbanksicherung wieder her.
2. Wendet alle gesicherten Transaktionsprotokolle sowie alle neuen Protokolle an, die seit der letzten Sicherung erstellt wurden.

Transaktionsprotokolle werden weitergeleitet und auf alle ausgewählten Datenbanken angewendet.

Exchange erstellt nach Abschluss einer Wiederherstellung eine neue Protokollkette.

**Best Practice:** Es wird empfohlen, nach Abschluss einer Wiederherstellung eine neue vollständige Sicherung und Protokollsicherung durchzuführen.

Für einen minutengenauen Wiederherstellungsvorgang ist ein zusammenhängender Satz von Transaktionsprotokollen erforderlich.

Nachdem Sie eine minutengenaue Wiederherstellung durchgeführt haben, ist die für die Wiederherstellung verwendete Sicherung nur für zeitpunktbezogene Wiederherstellungsvorgänge verfügbar.

Wenn Sie nicht für alle Sicherungen die Wiederherstellungsfunktion auf die Minute genau benötigen, können Sie die Aufbewahrungsdauer der Transaktionsprotokollsicherungen Ihres Systems über die Sicherungsrichtlinien konfigurieren.

### Wiederherstellen eines früheren Zeitpunkts

Bei einer zeitpunktbezogenen Wiederherstellung werden Datenbanken nur auf einen bestimmten Zeitpunkt in der Vergangenheit wiederhergestellt. Eine zeitpunktbezogene Wiederherstellung erfolgt in den folgenden Wiederherstellungssituationen:

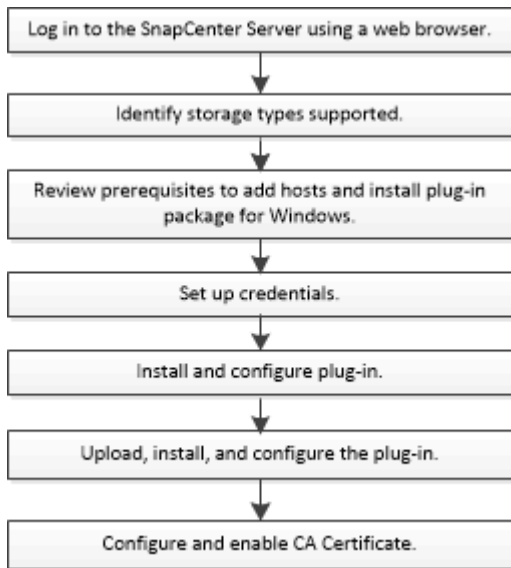
- Die Datenbank wird zu einem bestimmten Zeitpunkt in einem gesicherten Transaktionsprotokoll wiederhergestellt.
- Die Datenbank wird wiederhergestellt und nur eine Teilmenge der gesicherten Transaktionsprotokolle wird darauf angewendet.

## Installieren Sie das SnapCenter -Plug-in für Microsoft Exchange Server

### Installationsablauf des SnapCenter Plug-ins für Microsoft Exchange Server

Sie sollten das SnapCenter Plug-in für Microsoft Exchange Server installieren und

einrichten, wenn Sie Exchange-Datenbanken schützen möchten.



## Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für Microsoft Exchange Server

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Sie müssen Microsoft Exchange Server 2013, 2016 oder 2019 für eigenständige und Datenbankverfügbarkeitsgruppenkonfigurationen verwenden.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Wenn Sie Clusterknoten in SnapCenter verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Knoten im Cluster.
- Sie müssen über einen Benutzer mit Administratorberechtigungen auf dem Exchange-Server verfügen.
- Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, müssen Sie die Registrierung des von SnapDrive für Windows verwendeten VSS-Hardwareanbieters aufheben, bevor Sie das Plug-in für Exchange auf demselben Exchange Server installieren, um einen erfolgreichen Datenschutz mit SnapCenter sicherzustellen.
- Wenn SnapManager für Microsoft Exchange Server und Plug-in für Exchange auf demselben Server installiert sind, müssen Sie alle von SnapManager für Microsoft Exchange Server erstellten Zeitpläne aus dem Windows-Scheduler aussetzen oder löschen.
- Der Host muss vom Server aus in den vollqualifizierten Domännennamen (FQDN) auflösbar sein. Wenn die Hosts-Datei geändert wird, um sie auflösbar zu machen, und wenn sowohl der Kurzname als auch der FQDN in der Hosts-Datei angegeben sind, erstellen Sie einen Eintrag in der SnapCenter -Hosts-Datei im folgenden Format: `<IP-Adresse> <Host-FQDN> <Hostname>`.
- Stellen Sie sicher, dass die folgenden Ports in der Firewall nicht blockiert sind, da sonst der Vorgang zum Hinzufügen des Hosts fehlschlägt. Um dieses Problem zu beheben, müssen Sie den dynamischen

Portbereich konfigurieren. Weitere Informationen finden Sie unter ["Microsoft-Dokumentation"](#) .

- Portbereich 50000 – 51000 für Windows 2016 und Exchange 2016
- Portbereich 6000 – 6500 für Windows 2012 R2 und Exchange 2013
- Portbereich 49152 – 65536 für Windows 2019



Um den Portbereich zu identifizieren, führen Sie die folgenden Befehle aus:

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | Microsoft Windows<br><br>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .                                                                                                                                                                                                                                                                                                                             |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | 5 GB<br><br> 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 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java und OpenJDK</li> </ul> <p>Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

### Exchange Server-Berechtigungen erforderlich

Damit SnapCenter Exchange Server oder DAG hinzufügen und das SnapCenter Plug-in für Microsoft Exchange Server auf einem Host oder DAG installieren kann, müssen Sie SnapCenter mit Anmeldeinformationen für einen Benutzer mit einem Mindestsatz an Berechtigungen und Berechtigungen konfigurieren.

Sie benötigen einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remote-Exchange-Host sowie Administratorberechtigungen auf allen Knoten in der DAG. Der Domänenbenutzer benötigt die folgenden Mindestberechtigungen:

- Hinzufügen-MailboxDatabaseCopy
- Dismount-Datenbank
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Verschieben-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- Mount-Datenbank
- Neue Mailbox-Datenbank
- Neue PublicFolderDatabase
- Entfernen-MailboxDatabase
- Entfernen-MailboxDatabaseCopy

- Entfernen-PublicFolderDatabase
- Lebenslauf-MailboxDatenbankkopie
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                                                                                                                                                                          |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>5 GB</p> <div>  <p>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.</p> </div> |

| Artikel                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Erforderliche Softwarepakete | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java und OpenJDK</li> </ul> <p>Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

## Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für Windows

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation des Plug-In-Pakets und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen an Datenbanken erstellen.

### Informationen zu diesem Vorgang

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Windows-Hosts einrichten. Obwohl Sie Anmeldeinformationen für Windows erstellen können, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, empfiehlt es sich, die Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

Richten Sie die Anmeldeinformationen mit Administratorrechten ein, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.

Das Fenster „Anmeldeinformationen“ wird angezeigt.

4. Gehen Sie auf der Seite „Anmeldeinformationen“ wie folgt vor:



| Für dieses Feld...      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Benutzername            | <p>Geben Sie den Benutzernamen ein, der für die Authentifizierung verwendet wird.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: UserName</p> |
| Passwort                | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Authentifizierung       | Wählen Sie Windows als Authentifizierungsmodus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

5. Klicken Sie auf **OK**.

## Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

## Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -EffectivelImmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$  
.. Fügen Sie der Gruppe Computerobjekte hinzu.  
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu  
erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des  
Dienstkontos.
```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:
  - a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                   |
|---------|----------------|-----------|--------------------------------------------------|
| -----   | -----          | -----     | -----                                            |
| True    | No             | Success   | {Active Directory Domain Services,<br>Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Starten Sie Ihren Host neu.
  - b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
  - c. Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
  6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Hosts hinzufügen und Plug-in für Exchange installieren

Sie können die SnapCenter -Seite „Host hinzufügen“ verwenden, um Windows-Hosts hinzuzufügen. Das Plug-in für Exchange wird automatisch auf dem angegebenen Host installiert. Dies ist die empfohlene Methode zum Installieren von Plug-Ins. Sie können einen Host hinzufügen und ein Plug-In entweder für einen einzelnen Host oder einen Cluster installieren.

### Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise der SnapCenter Administrator.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Der Nachrichtenwarteschlangendienst muss ausgeführt werden.
- Wenn Sie ein gruppenveraltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren. Weitere Informationen finden Sie unter ["Konfigurieren Sie ein gruppenveraltetes Dienstkonto auf Windows Server 2016 oder höher für Microsoft Exchange Server"](#).

### Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder einen Cluster installieren.
- Wenn ein Exchange-Knoten Teil einer DAG ist, können Sie nicht nur einen Knoten zum SnapCenter -Server hinzufügen.
- Wenn Sie Plug-Ins auf einem Cluster (Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert, auch wenn einige Knoten keine Datenbanken auf NetApp LUNs haben.

Ab SnapCenter 4.6 unterstützt SCE Mandantenfähigkeit und Sie können einen Host mit den folgenden

Methoden hinzufügen:

| Hostvorgang hinzufügen                                                                                             | 4.5 und früher    | 4.6 und höher |
|--------------------------------------------------------------------------------------------------------------------|-------------------|---------------|
| Fügen Sie einen IP-losen DAG in einer anderen oder einer anderen Domäne hinzu                                      | Nicht unterstützt | Unterstützt   |
| Fügen Sie mehrere IP-DAGs mit eindeutigen Namen hinzu, die sich in derselben oder einer anderen Domäne befinden.   | Unterstützt       | Unterstützt   |
| Fügen Sie mehrere IP- oder IP-lose DAGs hinzu, die denselben Hostnamen und/oder DB-Namen domänenübergreifend haben | Nicht unterstützt | Unterstützt   |
| Fügen Sie mehrere IP/IP-lose DAGs mit demselben Namen und domänenübergreifend hinzu                                | Nicht unterstützt | Unterstützt   |
| Fügen Sie mehrere eigenständige Hosts mit demselben Namen und domänenübergreifend hinzu                            | Nicht unterstützt | Unterstützt   |

Das Plug-in für Exchange hängt vom SnapCenter Plug-in-Paket für Windows ab und die Versionen müssen identisch sein. Während der Installation des Plug-ins für Exchange wird standardmäßig das SnapCenter Plug-ins-Paket für Windows ausgewählt und zusammen mit dem VSS-Hardwareanbieter installiert.

Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind und Sie das Plug-in für Exchange auf demselben Exchange Server installieren möchten, müssen Sie die Registrierung des von SnapDrive für Windows verwendeten VSS-Hardwareanbieters aufheben, da dieser nicht mit dem VSS-Hardwareanbieter kompatibel ist, der mit dem Plug-in für Exchange und dem SnapCenter Plug-ins Package für Windows installiert wurde. Weitere Informationen finden Sie unter ["So registrieren Sie den Data ONTAP VSS Hardware Provider manuell"](#) .

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Gehen Sie auf der Seite „Hosts“ wie folgt vor:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosttyp            | <p data-bbox="841 157 1268 191">Wählen Sie <b>Windows</b> als Hosttyp.</p> <p data-bbox="841 224 1471 357">SnapCenter Server fügt den Host hinzu und installiert dann auf dem Host das Plug-in für Windows und das Plug-in für Exchange, falls diese noch nicht installiert sind.</p> <p data-bbox="841 392 1487 560">Plug-in für Windows und Plug-in für Exchange müssen dieselbe Version haben. Wenn zuvor eine andere Version des Plug-ins für Windows installiert war, aktualisiert SnapCenter die Version im Rahmen der Installation.</p> |

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hostname</p>    | <p>Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.</p> <p>SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den vollqualifizierten Domännennamen (FQDN) einzugeben.</p> <p>Eine IP-Adresse wird für nicht vertrauenswürdige Domänenhosts nur unterstützt, wenn sie in den FQDN aufgelöst wird.</p> <p>Wenn Sie mit SnapCenter einen Host hinzufügen und dieser Teil einer Subdomäne ist, müssen Sie den FQDN angeben.</p> <p>Sie können IP-Adressen oder den FQDN eines der folgenden Elemente eingeben:</p> <ul style="list-style-type: none"> <li>• Eigenständiger Host</li> <li>• DAG austauschen</li> </ul> <p>Für einen Exchange-DAG können Sie:</p> <ul style="list-style-type: none"> <li>◦ Fügen Sie einen DAG hinzu, indem Sie den DAG-Namen, die DAG-IP-Adresse, den Knotennamen oder die Knoten-IP-Adresse angeben.</li> <li>◦ Fügen Sie den IP-losen DAG-Cluster hinzu, indem Sie die IP-Adresse oder den FQDN eines der DAG-Clusterknoten angeben.</li> <li>◦ Fügen Sie einen DAG ohne IP hinzu, der sich in derselben oder einer anderen Domäne befindet. Sie können auch mehrere IP/IP-lose DAGs mit demselben Namen, aber unterschiedlichen Domänen hinzufügen.</li> </ul> <div>  <p>Für einen eigenständigen Host oder einen Exchange-DAG (domänenübergreifend oder dieselbe Domäne) wird empfohlen, den FQDN oder die IP-Adresse des Hosts oder DAG anzugeben.</p> </div> |

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

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

Wenn Sie „Plug-in für Exchange“ auswählen, wird die Auswahl von „SnapCenter Plug-in für Microsoft SQL Server“ automatisch aufgehoben. Microsoft empfiehlt, SQL Server und Exchange Server aufgrund der Speicherbelegung und anderer von Exchange benötigter Ressourcennutzung nicht auf demselben System zu installieren.

6. (Optional) Klicken Sie auf **Weitere Optionen**.

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen              | <p>Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an.</p> <p>Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installationspfad                                                                           | Der Standardpfad ist <code>C:\Program Files\NetApp\SnapCenter</code> .<br><br>Optional können Sie den Pfad anpassen.                                                                                                                                                                                                                                                                                                                                                 |
| Alle Hosts in der DAG hinzufügen                                                            | Aktivieren Sie dieses Kontrollkästchen, wenn Sie einen DAG hinzufügen.                                                                                                                                                                                                                                                                                                                                                                                               |
| Vorinstallationsprüfungen überspringen                                                      | 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.                                                                                                                                                                                                                                                               |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | Aktivieren Sie dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.<br><br>Geben Sie den gMSA-Namen im folgenden Format an: <code>Domänenname\Kontoname\$</code> .<br><br><div>  <div>gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.</div> </div> |

#### 7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Voraussetzungen für die Installation des Plug-Ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei `web.config` aktualisieren, die sich unter `C:\Program Files\NetApp\SnapCenter WebApp` zum Ändern der Standardwerte. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.



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

#### 8. Überwachen Sie den Installationsfortschritt.

### Konfigurieren Sie einen benutzerdefinierten Port für die NET TCP-Kommunikation

Ab der SnapCenter Version 6.0 verwendet das SnapCenter -Plug-in für Windows standardmäßig den Port 909 für die NET TCP-Kommunikation. Wenn der Port 909 verwendet wird, können Sie einen anderen Port für die NET TCP-Kommunikation konfigurieren.



## Schritte

1. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config* in die erforderliche Portnummer.  
`<add key="NetTCPPort" value="new_port_number" />`
2. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Programme\NetApp\SnapCenter\SnapCenter Plug-in für Microsoft Windows\SnapDriveService.dll.config* in die erforderliche Portnummer.  
`<add key="NetTCPPort" value="new_port_number" />`
3. Heben Sie die Registrierung des Dienstes *Data ONTAP VSS Hardware Provider* auf, indem Sie den folgenden Befehl ausführen:  
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`  
  
Stellen Sie sicher, dass der Dienst nicht in der Liste der Dienste in *services.msc* angezeigt wird.
4. Registrieren Sie den Dienst *Data ONTAP VSS Hardware Provider*, indem Sie den folgenden Befehl ausführen:  
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`  
  
Überprüfen Sie, ob der Dienst jetzt in der Liste der Dienste in *services.msc* angezeigt wird.
5. Starten Sie den Dienst „Plug-in für Windows“ neu.

## Installieren Sie das Plug-in für Exchange vom SnapCenter Server-Host mithilfe von PowerShell-Cmdlets

Sie sollten das Plug-in für Exchange über die SnapCenter -GUI installieren. Wenn Sie die GUI nicht verwenden möchten, können Sie PowerShell-Cmdlets auf dem SnapCenter Server-Host oder auf einem Remote-Host verwenden.

### Bevor Sie beginnen

- SnapCenter Server muss installiert und konfiguriert sein.
- Sie müssen ein lokaler Administrator auf dem Host oder ein Benutzer mit Administratorrechten sein.
- Sie müssen ein Benutzer sein, dem eine Rolle mit Plug-In-, Installations- und Deinstallationsberechtigungen zugewiesen ist, beispielsweise der SnapCenter Administrator.
- Sie müssen die Installationsanforderungen und die unterstützten Konfigurationstypen überprüft haben, bevor Sie das Plug-in für Exchange installieren.
- Der Host, auf dem Sie das Plug-in für Exchange installieren möchten, muss ein Windows-Host sein.

## Schritte

1. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
2. Fügen Sie den Host hinzu, auf dem Sie das Plug-in für Exchange installieren möchten, indem Sie das Cmdlet *Add-SmHost* mit den erforderlichen Parametern verwenden.

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"](#) .

Der Host kann ein eigenständiger Host oder ein DAG sein. Wenn Sie einen DAG angeben, ist der

Parameter *-IsDAG* erforderlich.

3. Installieren Sie das Plug-in für Exchange mithilfe des Cmdlets *Install-SmHostPackage* mit den erforderlichen Parametern.

Dieser Befehl installiert das Plug-in für Exchange auf dem angegebenen Host und registriert das Plug-in dann bei SnapCenter.

## Installieren Sie das SnapCenter -Plug-in für Exchange im Hintergrund über die Befehlszeile

Sie sollten das Plug-in für Exchange über die SnapCenter -Benutzeroberfläche installieren. Wenn dies aus irgendeinem Grund nicht möglich ist, können Sie das Plug-in für Exchange-Installationsprogramm unbeaufsichtigt im Hintergrundmodus über die Windows-Befehlszeile ausführen.

### Bevor Sie beginnen

- Sie müssen Ihre Microsoft Exchange Server-Ressourcen gesichert haben.
- Sie müssen die SnapCenter Plug-In-Pakete installiert haben.
- Sie müssen die frühere Version des SnapCenter -Plug-ins für Microsoft SQL Server vor der Installation löschen.

Weitere Informationen finden Sie unter ["So installieren Sie ein SnapCenter -Plug-In manuell und direkt vom Plug-In-Host"](#) .

### Schritte

1. Überprüfen Sie, ob der Ordner *C:\temp* auf dem Plug-In-Host vorhanden ist und der angemeldete Benutzer vollen Zugriff darauf hat.
2. Laden Sie das SnapCenter -Plug-in für Microsoft Windows von *C:\ProgramData\NetApp\SnapCenter\Package Repository* herunter.

Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

3. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-In installieren möchten.
4. Navigieren Sie von einer Windows-Eingabeaufforderung auf dem lokalen Host zu dem Verzeichnis, in dem Sie die Plug-In-Installationsdateien gespeichert haben.
5. Geben Sie den folgenden Befehl ein, um das Plug-In zu installieren.

```
snapcenter_windows_host_plugin.exe"/silent /debuglog"<Debug_Log_Path>" /log"<Log_Path>"  
BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Install_Directory_Pfad>"  
BI_SERVICEACCOUNT=<Domäne\Administrator> BI_SERVICEPWD=<Passwort>  
ISFeatureInstall=HPPW,SCW,SCE
```

Beispiel:

```
C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe"/silent  
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Programme\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=Domäne\Administrator BI_SERVICEPWD=Passwort  
ISFeatureInstall=HPPW,SCW,SCE
```



Bei allen während der Installation des Plug-ins für Exchange übergebenen Parametern wird zwischen Groß- und Kleinschreibung unterschieden.

Geben Sie für die Variablen folgende Werte ein:

| Variable                                      | Wert                                                                                                                                                                                                                     |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/debuglog"&lt;Debug_Log_Pfad&gt;</code> | Geben Sie den Namen und den Speicherort der Protokolldatei des Suite-Installationsprogramms an, wie im folgenden Beispiel:<br><br><code>Setup.exe</code><br><code>/debuglog"C:\PfadZurProtokolldatei\setupexe.log</code> |
| <code>BI_SNAPCENTER_PORT</code>               | Geben Sie den Port an, über den SnapCenter mit SMCORE kommuniziert.                                                                                                                                                      |
| <code>SUITE_INSTALLDIR</code>                 | Geben Sie das Installationsverzeichnis des Host-Plug-In-Pakets an.                                                                                                                                                       |
| <code>BI_SERVICEACCOUNT</code>                | Geben Sie das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.                                                                                                                                            |
| <code>BI_SERVICEPWD</code>                    | Geben Sie das Kennwort für das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.                                                                                                                           |
| <code>ISFeatureInstall</code>                 | Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host bereitgestellt werden soll.                                                                                                                              |

- Überwachen Sie den Windows-Taskplaner, die Hauptinstallationsprotokolldatei `C:\Installdebug.log` und die zusätzlichen Installationsdateien in `C:\Temp`.
- Überwachen Sie das Verzeichnis `%temp%`, um zu überprüfen, ob die `msiexe.exe`-Installationsprogramme die Software ohne Fehler installieren.



Bei der Installation des Plug-ins für Exchange wird das Plug-in auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie können das Plug-In auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder des PowerShell-Cmdlets hinzufügen. Nachdem der Host hinzugefügt wurde, wird das Plug-In automatisch erkannt.

## Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#) .



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

## CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

## Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.

- b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
- c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
- d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
- e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

## 2. Führen Sie in PowerShell Folgendes aus:

- a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-Childitem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

## Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-
in-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## 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.

## Konfigurieren Sie SnapManager 7.x für die Koexistenz von Exchange und SnapCenter

Damit das SnapCenter -Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server gleichzeitig verwendet werden können, müssen Sie das SnapCenter -Plug-in für Microsoft Exchange Server auf demselben Exchange Server

installieren, auf dem SnapManager für Microsoft Exchange Server installiert ist, die Zeitpläne von SnapManager für Exchange deaktivieren und neue Zeitpläne und Sicherungen mithilfe des SnapCenter -Plug-ins für Microsoft Exchange Server konfigurieren.

### Bevor Sie beginnen

- SnapManager für Microsoft Exchange Server und SnapDrive für Windows sind bereits installiert und SnapManager für Microsoft Exchange Server-Backups sind auf dem System und im SnapInfo-Verzeichnis vorhanden.
- Sie sollten die von SnapManager für Microsoft Exchange Server erstellten Backups, die Sie nicht mehr benötigen, gelöscht oder wiederhergestellt haben.
- Sie sollten alle von SnapManager für Microsoft Exchange Server erstellten Zeitpläne aus dem Windows-Planer angehalten oder gelöscht haben.
- SnapCenter Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server können auf demselben Exchange Server koexistieren, Sie können jedoch vorhandene SnapManager für Microsoft Exchange Server-Installationen nicht auf SnapCenter aktualisieren.

SnapCenter bietet keine Option für das Upgrade.

- SnapCenter unterstützt nicht die Wiederherstellung von Exchange-Datenbanken aus SnapManager für Microsoft Exchange Server-Backups.

Wenn Sie SnapManager für Microsoft Exchange Server nach der Installation des SnapCenter -Plug-ins für Microsoft Exchange Server nicht deinstallieren und später ein SnapManager für Microsoft Exchange Server-Backup wiederherstellen möchten, müssen Sie zusätzliche Schritte ausführen.

### Schritte

1. Ermitteln Sie mithilfe von PowerShell auf allen DAG-Knoten, ob der SnapDrive für Windows VSS-Hardwareanbieter registriert ist: *vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. Heben Sie im SnapDrive -Verzeichnis die Registrierung des VSS-Hardwareanbieters von SnapDrive für Windows auf: *navssprv.exe -r service -u*
3. Überprüfen Sie, ob der VSS-Hardwareanbieter entfernt wurde: *vssadmin list providers*
4. Fügen Sie den Exchange-Host zu SnapCenter hinzu und installieren Sie dann das SnapCenter -Plug-in für Microsoft Windows und das SnapCenter -Plug-in für Microsoft Exchange Server.
5. Überprüfen Sie im Verzeichnis „SnapCenter Plug-in für Microsoft Windows“ auf allen DAG-Knoten, ob der VSS-Hardwareanbieter registriert ist: *vssadmin list providers*



```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
Version: 7. 0. 0. 5561
```

6. Stoppen Sie die Sicherungspläne von SnapManager für Microsoft Exchange Server.
7. Erstellen Sie mithilfe der SnapCenter -GUI On-Demand-Backups, konfigurieren Sie geplante Backups und konfigurieren Sie Aufbewahrungseinstellungen.
8. Deinstallieren Sie SnapManager für Microsoft Exchange Server.

Wenn Sie SnapManager für Microsoft Exchange Server jetzt nicht deinstallieren und später ein SnapManager für Microsoft Exchange Server-Backup wiederherstellen möchten:

- a. Heben Sie die Registrierung des SnapCenter -Plug-ins für Microsoft Exchange Server von allen DAG-Knoten auf: *navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. Registrieren Sie SnapDrive für Windows im Verzeichnis *C:\Programme\NetApp\SnapDrive \* auf allen DAG-Knoten: *navssprv.exe -r service -a hostname\username -p password*

## 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 Datenschutz vor

Bevor Sie Datenschutzvorgänge wie Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen, müssen Sie Ihre Strategie definieren und die 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.

### Weitere Informationen finden

["Erste Schritte mit der REST-API"](#)

## Voraussetzungen für die Verwendung des SnapCenter Plug-Ins für Microsoft Exchange Server

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

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich bei SnapCenter an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen oder zuweisen und Anmeldeinformationen erstellen.



SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss einen eindeutigen Namen haben.

- Fügen Sie Hosts hinzu, installieren Sie das SnapCenter -Plug-in für Microsoft Windows und das SnapCenter -Plug-in für Microsoft Exchange Server und ermitteln (aktualisieren) Sie die Ressourcen.
- Führen Sie die hostseitige Speicherbereitstellung mit dem SnapCenter -Plug-in für Microsoft Windows durch.
- Wenn Sie SnapCenter Server zum Schutz von Exchange-Datenbanken verwenden, die sich auf VMware RDM LUNs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Weitere Informationen finden Sie in der Dokumentation zum SnapCenter Plug-in for VMware vSphere .



VMDKs werden nicht unterstützt.

- Verschieben Sie eine vorhandene Microsoft Exchange Server-Datenbank mithilfe von Microsoft Exchange-Tools von einer lokalen Festplatte auf einen unterstützten Speicher.
- Richten Sie SnapMirror und SnapVault -Beziehungen ein, wenn Sie eine Backup-Replikation wünschen.

Für Benutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.1.1 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme. Für Benutzer von SnapCenter 4.2.x sowie NetApp Data Broker 1.0 und 1.0.1 enthält die Dokumentation Informationen zum Schutz

virtualisierter Datenbanken und Dateisysteme mithilfe des SnapCenter Plug-in for VMware vSphere, das von der Linux-basierten virtuellen NetApp Data Broker-Appliance (Open Virtual Appliance-Format) bereitgestellt wird. Für Benutzer von SnapCenter 4.3.x enthält die Dokumentation zum SnapCenter Plug-in for VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des Linux-basierten SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance-Format).

["SnapCenter Plug-in for VMware vSphere Dokumentation"](#)

## **So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von Exchange Server verwendet**

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Wiederherstellungs- und Reseed-Vorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei den Ressourcen handelt es sich in der Regel um Postfachdatenbanken oder Microsoft Exchange Database Availability Groups (DAGs), die Sie mit SnapCenter sichern.
- Eine SnapCenter -Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG und die Ressourcengruppe kann entweder einen ganzen DAG oder einzelne Datenbanken umfassen.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

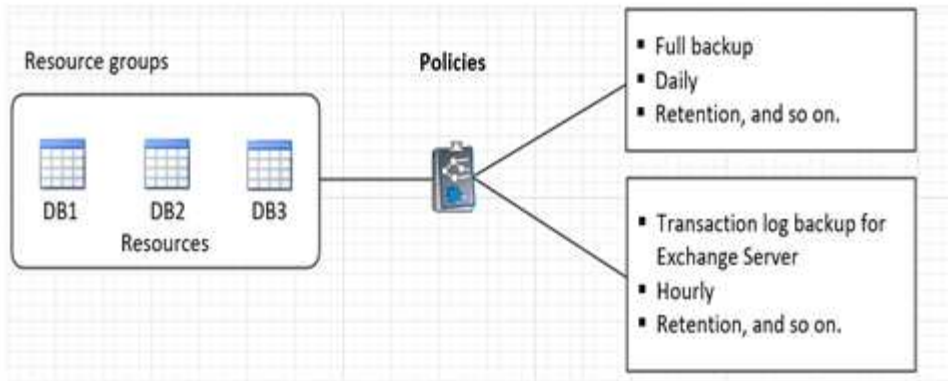
Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

Die Ressourcengruppen wurden früher als Datensätze bezeichnet.

- Die Richtlinien legen die Sicherungshäufigkeit, die Aufbewahrung von Kopien, Skripts und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine oder mehrere Richtlinien auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

Stellen Sie sich eine Ressourcengruppe so vor, als würde sie definieren, *was* Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als würde sie definieren, *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anfügen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird, und einen anderen Zeitplan, der stündlich Protokollsicherungen durchführt. Die folgende Abbildung veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



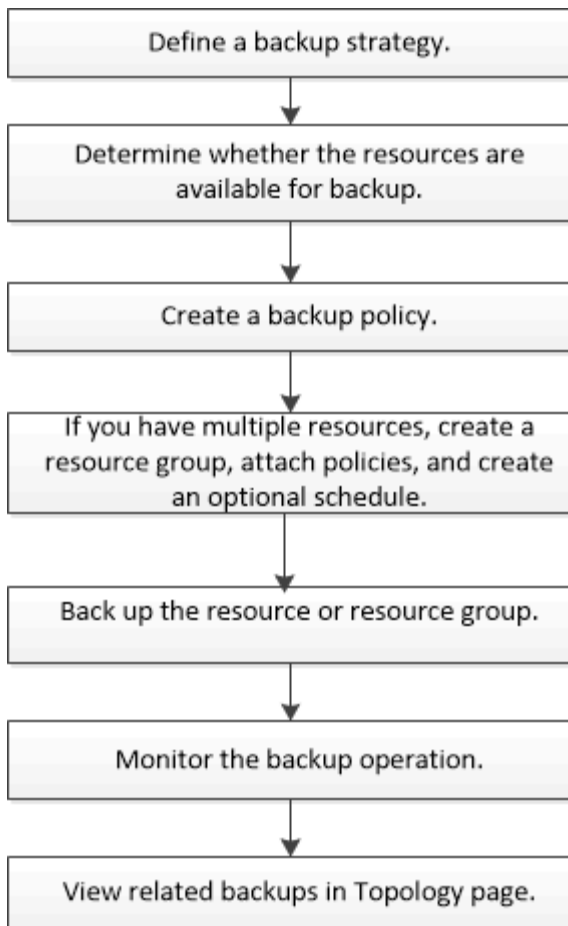
## Sichern von Exchange-Ressourcen

### Sicherungsworkflow

Wenn Sie das SnapCenter -Plug-in für Microsoft Exchange Server in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern von Exchange-Ressourcen verwenden.

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden. Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden. Aktive und passive Sicherungskopien auf demselben Volume werden nicht unterstützt.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



## Exchange-Datenbank und Backup-Verifizierung

Das SnapCenter -Plug-in für Microsoft Exchange Server bietet keine Sicherungsüberprüfung. Sie können jedoch das mit Exchange bereitgestellte Tool „Eseutil“ verwenden, um Exchange-Datenbanken und -Sicherungen zu überprüfen.

Das Microsoft Exchange Eseutil-Tool ist ein Befehlszeilenprogramm, das in Ihrem Exchange-Server enthalten ist. Mit dem Dienstprogramm können Sie Konsistenzprüfungen durchführen, um die Integrität von Exchange-Datenbanken und -Sicherungen zu überprüfen.

**Best Practice:** Es ist nicht notwendig, Konsistenzprüfungen für Datenbanken durchzuführen, die Teil einer Database Availability Group (DAG)-Konfiguration mit mindestens zwei Replikaten sind.

Weitere Informationen finden Sie unter ["Microsoft Exchange Server-Dokumentation"](#).

## Ermitteln, ob Exchange-Ressourcen für die Sicherung verfügbar sind

Ressourcen sind die Datenbanken und Exchange Database Availability Groups, die von den von Ihnen installierten Plug-Ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzaufgaben auszuführen. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Ihnen zur Verfügung stehen. Durch die Ermittlung der verfügbaren Ressourcen wird auch überprüft, ob die Plug-In-Installation erfolgreich abgeschlossen wurde.

## Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen, das Hinzufügen von Anmeldeinformationen und die Installation des Plug-ins für Exchange abgeschlossen haben.
- Um die Funktionen der Single Mailbox Recovery-Software nutzen zu können, müssen Sie Ihre aktive Datenbank auf dem Exchange-Server lokalisiert haben, auf dem die Single Mailbox Recovery-Software installiert ist.
- Wenn sich Datenbanken auf VMware RDM LUNs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Der "[SnapCenter Plug-in for VMware vSphere Dokumentation](#)" hat weitere Informationen.

## Informationen zu diesem Vorgang

- Sie können keine Datenbanken sichern, wenn die Option **Gesamtstatus** auf der Seite „Details“ auf „Nicht für Sicherung verfügbar“ eingestellt ist. Die Option **Gesamtstatus** wird auf „Nicht für Sicherung verfügbar“ gesetzt, wenn eine der folgenden Bedingungen zutrifft:
  - Datenbanken befinden sich nicht auf einer NetApp LUN.
  - Die Datenbanken befinden sich nicht im Normalzustand.

Datenbanken befinden sich nicht im Normalzustand, wenn sie sich im Status „Mounten“, „Unmounten“, „Reseed“ oder „Wiederherstellung ausstehend“ befinden.

- Wenn Sie über eine Database Availability Group (DAG) verfügen, können Sie alle Datenbanken in der Gruppe sichern, indem Sie den Sicherungsauftrag von der DAG aus ausführen.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **Microsoft Exchange Server** aus der Plug-In-Dropdownliste in der oberen linken Ecke der Ressourcenseite aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdownliste „Anzeigen“ die Option „**Datenbank**“, „**Datenbankverfügbarkeitsgruppe**“ oder „**Ressourcengruppe**“ aus.

Alle Datenbanken und DAGs werden mit ihren DAG- oder Hostnamen im FQDN-Format angezeigt, sodass Sie zwischen mehreren Datenbanken unterscheiden können.

Klicken  und wählen Sie den Hostnamen und den Exchange-Server aus, um die Ressourcen zu filtern. Sie können dann auf , um den Filterbereich zu schließen.

3. Klicken Sie auf **Ressourcen aktualisieren**.

Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden im SnapCenter Server-Inventar aktualisiert.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Die Ressourcen werden zusammen mit Informationen wie Ressourcenname, Name der Datenbankverfügbarkeitsgruppe, Server, auf dem die Datenbank derzeit aktiv ist, Server mit Kopien, Zeitpunkt der letzten Sicherung und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem Nicht- NetApp -Speicher befindet, wird in der Spalte „Gesamtstatus“ „Nicht für Sicherung verfügbar“ angezeigt.

Wenn sich in einer DAG die aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und sich mindestens eine passive Datenbankkopie auf einem NetApp -Speicher befindet, wird in der Spalte **Gesamtstatus** „Nicht geschützt“ angezeigt.

Sie können keine Datenschutzvorgänge für eine Datenbank durchführen, die sich auf einem anderen Speichertyp als NetApp befindet.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte **Gesamtstatus** „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte **Gesamtstatus** die Meldung „Sicherung nicht ausgeführt“ an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist und die Sicherung für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche in der Spalte **Gesamtstatus** die Meldung „Sicherung erfolgreich“ an.

## Erstellen von Sicherungsrichtlinien für Exchange Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Exchange-Ressourcen oder für die Ressourcengruppen erstellen, bevor Sie SnapCenter zum Sichern von Microsoft Exchange Server-Ressourcen verwenden, oder Sie können eine Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine einzelne Ressource sichern.

### Bevor Sie beginnen

- Sie müssen Ihre Datenschutzstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für Exchange-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Sie müssen die Exchange Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss der SnapCenter Administrator Ihnen die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des `usePowershellProcessforScripts` Parameter auf `true` im `web.config` Datei.

Der Standardwert ist „false“.

- 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

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten und aufbewahren und wie häufig die Ressource oder Ressourcengruppe gesichert wird. Darüber hinaus können Sie Skripteinstellungen festlegen. Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.
- Die vollständige Aufbewahrung von Backups ist an eine bestimmte Richtlinie gebunden. Eine Datenbank

oder Ressource, die Richtlinie A mit einer vollständigen Sicherungsaufbewahrung von 4 verwendet, behält 4 vollständige Sicherungen bei und hat keine Auswirkungen auf Richtlinie B für dieselbe Datenbank oder Ressource, die möglicherweise eine Aufbewahrung von 3 hat, um 3 vollständige Sicherungen beizubehalten.

- Die Aufbewahrung von Protokollsicherungen ist richtlinienübergreifend wirksam und gilt für alle Protokollsicherungen einer Datenbank oder Ressource. Wenn also eine vollständige Sicherung mit Richtlinie B durchgeführt wird, wirkt sich die Protokollaufbewahrungseinstellung auf Protokollsicherungen aus, die mit Richtlinie A auf derselben Datenbank oder Ressource erstellt wurden. Ebenso wirkt sich die Protokollaufbewahrungseinstellung für Richtlinie A auf Protokollsicherungen aus, die von Richtlinie B in derselben Datenbank erstellt wurden.
- Der `SCRIPTS_PATH` wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: `API /4.7/configsettings`

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

**Best Practice:** Am besten konfigurieren Sie die sekundäre Aufbewahrungsrichtlinie basierend auf der Anzahl der vollständigen und Protokollsicherungen, die Sie insgesamt aufbewahren möchten. Wenn Sie sekundäre Aufbewahrungsrichtlinien konfigurieren, bedenken Sie, dass bei Datenbanken und Protokollen, die sich auf unterschiedlichen Volumes befinden, jede Sicherung drei Snapshots haben kann, und dass bei Datenbanken und Protokollen, die sich auf demselben Volume befinden, jede Sicherung zwei Snapshots haben kann.

- 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 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. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Sicherungstyp und Replikation“ die folgenden Schritte aus:
  - a. Wählen Sie den Sicherungstyp:



| Wenn Sie wollen...                                                                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sichern Sie die Datenbankdateien und die erforderlichen Transaktionsprotokolle                                | <p>Wählen Sie <b>Vollständige Sicherung und Protokollsicherung</b>.</p> <p>Datenbanken werden mit Protokollkürzung gesichert und alle Protokolle werden gesichert, einschließlich der gekürzten Protokolle.</p> <div>  <p>Dies ist der empfohlene Sicherungstyp.</p> </div>                                                                                            |
| Sichern Sie die Datenbankdateien und die nicht festgeschriebenen Transaktionsprotokolle                       | <p>Wählen Sie <b>Vollständige Sicherung</b>.</p> <p>Datenbanken werden mit Protokollkürzung gesichert, gekürzte Protokolle werden nicht gesichert.</p>                                                                                                                                                                                                                                                                                                  |
| Sichern Sie alle Transaktionsprotokolle                                                                       | <p>Wählen Sie <b>Protokollsicherung</b>.</p> <p>Alle Transaktionsprotokolle auf dem aktiven Dateisystem werden gesichert und es erfolgt keine Protokollkürzung.</p> <p>Auf derselben Festplatte wie das Live-Protokoll wird ein <i>scebackupinfo</i>-Verzeichnis erstellt. Dieses Verzeichnis enthält den Zeiger auf die inkrementellen Änderungen für die Exchange-Datenbank und ist nicht gleichbedeutend mit den vollständigen Protokolldateien.</p> |
| Sichern Sie alle Datenbankdateien und Transaktionsprotokolle, ohne die Transaktionsprotokolldateien zu kürzen | <p>Wählen Sie <b>Backup kopieren</b>.</p> <p>Alle Datenbanken und alle Protokolle werden gesichert und es erfolgt keine Protokollkürzung. Normalerweise verwenden Sie diesen Sicherungstyp zum erneuten Seeding eines Replikats oder zum Testen oder Diagnostizieren eines Problems.</p>                                                                                                                                                                |



Sie sollten den für Protokollsicherungen erforderlichen Speicherplatz auf Grundlage der vollständigen Sicherungsaufbewahrung und nicht auf Grundlage der minutengenauen (UTM) Aufbewahrung definieren.



Erstellen Sie beim Umgang mit Exchange-Volumes (LUNs) separate Tresorrichtlinien für Protokolle und Datenbanken und legen Sie die Aufbewahrungsdauer (Keep) für die Protokollrichtlinie für jedes Label auf die doppelte Zahl fest wie für die Datenbankrichtlinie, wobei Sie dieselben Labels verwenden. Weitere Informationen finden Sie unter ["SnapCenter für Exchange-Backups speichert nur die Hälfte der Snapshots auf dem Vault-Zielprotokollvolume"](#)

b. Wählen Sie im Abschnitt „Einstellungen der Datenbankverfügbarkeitsgruppe“ eine Aktion aus:

| Für dieses Feld...                                                                                   | Machen Sie Folgendes...                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sichern aktiver Kopien                                                                               | <p>Wählen Sie diese Option, um nur die aktiven Kopien der ausgewählten Datenbank zu sichern.</p> <p>Bei Datenbankverfügbarkeitsgruppen (DAGs) sichert diese Option nur aktive Kopien aller Datenbanken in der DAG.</p> <p>Passive Kopien werden nicht gesichert.</p> |
| Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen | <p>Wählen Sie diese Option, um alle Kopien der Datenbanken auf den ausgewählten Servern (aktiv und passiv) zu sichern.</p> <p>Bei DAGs sichert diese Option sowohl aktive als auch passive Kopien aller Datenbanken auf den ausgewählten Servern.</p>                |



In Clusterkonfigurationen werden die Sicherungen gemäß den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Knoten des Clusters aufbewahrt. Wenn sich der Besitzerknoten des Clusters ändert, bleiben die Sicherungen des vorherigen Besitzerknotens erhalten. Die Aufbewahrung gilt nur auf Knotenebene.

c. Wählen Sie im Abschnitt „Häufigkeit planen“ einen oder mehrere der Häufigkeitstypen aus: **Auf Anfrage, Stündlich, Täglich, Wöchentlich** und **Monatlich**.



Sie können den Zeitplan (Startdatum, Enddatum) für Sicherungsvorgänge beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungspläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

a. 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.

b. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

| Für dieses Feld...                                                      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots | <p>Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) aufzubewahren.</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.</p> <div>  <p>Die Nur-Primär-Richtlinie kann nicht verwendet werden, wenn SnapMirror Active Sync für Exchange ONTAP -Volumes eingerichtet ist. SnapCenter lässt dies nicht zu. Sie sollten die Option „Spiegeln“ aktivieren.</p> </div> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“"</a> .</p> |
| Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots  | Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Fehleranzahl der Wiederholungsversuche                                  | Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

## 6. Konfigurieren Sie auf der Seite „Aufbewahrung“ die Aufbewahrungseinstellungen.

Die angezeigten Optionen hängen vom Sicherungstyp und der Häufigkeit ab, die Sie zuvor ausgewählt haben.



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.

- a. Wählen Sie im Abschnitt „Aufbewahrungseinstellungen für Protokollsicherungen“ eine der folgenden Optionen aus:

| Wenn Sie wollen...                                                     | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Behalten Sie nur eine bestimmte Anzahl von Protokollsicherungen</p> | <p>Wählen Sie <b>Anzahl der vollständigen Sicherungen, für die Protokolle aufbewahrt werden</b> und geben Sie die Anzahl der vollständigen Sicherungen an, für die Sie eine minutengenaue Wiederherstellung wünschen.</p> <p>Die minutengenaue Aufbewahrung (UTM) gilt für Protokollsicherungen, die über eine vollständige oder Protokollsicherung erstellt wurden. Wenn beispielsweise die UTM-Aufbewahrungseinstellungen so konfiguriert sind, dass die Protokollsicherungen der letzten 5 vollständigen Sicherungen aufbewahrt werden, werden die Protokollsicherungen der letzten 5 vollständigen Sicherungen aufbewahrt.</p> <p>Die im Rahmen von Voll- und Log-Backups erstellten Log-Ordner werden im Rahmen von UTM automatisch gelöscht. Sie können die Protokollordner nicht manuell löschen. Wenn beispielsweise die Aufbewahrungseinstellung für die vollständige oder vollständige und Protokollsicherung auf 1 Monat und die UTM-Aufbewahrung auf 10 Tage eingestellt ist, wird der im Rahmen dieser Sicherungen erstellte Protokollordner gemäß UTM gelöscht. Infolgedessen sind nur 10-Tage-Protokollordner vorhanden und alle anderen Sicherungen sind für die Wiederherstellung zu einem bestimmten Zeitpunkt markiert.</p> <p>Sie können den UTM-Aufbewahrungswert auf 0 setzen, wenn Sie keine minutengenaue Wiederherstellung durchführen möchten. Dadurch wird die Wiederherstellung zu einem bestimmten Zeitpunkt ermöglicht.</p> <p><b>Best Practice:</b> Es ist am besten, wenn die Einstellung der Einstellung für „Gesamtanzahl der Snapshots (vollständige Sicherungen)“ im Abschnitt „Einstellungen für die Aufbewahrung vollständiger Sicherungen“ entspricht. Dadurch wird sichergestellt, dass die Protokolldateien für jede vollständige Sicherung erhalten bleiben.</p> |

| Wenn Sie wollen...                                                        | Machen Sie Folgendes...                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bewahren Sie die Sicherungskopien für eine bestimmte Anzahl von Tagen auf | <p>Wählen Sie die Option <b>Protokollsicherungen bis zuletzt aufbewahren</b> und geben Sie die Anzahl der Tage an, für die die Protokollsicherungskopien aufbewahrt werden sollen.</p> <p>Die Protokollsicherungen werden bis zur Anzahl der Tage der vollständigen Sicherungen aufbewahrt.</p> |
| Snapshot-Sperrzeitraum                                                    | <p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopie</b> und wählen Sie Tage, Monate oder Jahre aus.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p>                                                                                                         |

Wenn Sie als Sicherungstyp **Protokollsicherung** ausgewählt haben, werden Protokollsicherungen als Teil der aktuellen Aufbewahrungseinstellungen für vollständige Sicherungen aufbewahrt.

- b. Wählen Sie im Abschnitt „Aufbewahrungseinstellungen für vollständige Sicherungen“ eine der folgenden Optionen für On-Demand-Sicherungen und dann eine für vollständige Sicherungen aus:

| Für dieses Feld...                                                   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie nur eine bestimmte Anzahl von Snapshots                 | <p>Wenn Sie die Anzahl der aufzubewahrenden Vollsicherungen angeben möchten, wählen Sie die Option <b>Gesamtzahl der aufzubewahrenden Snapshot-Kopien</b> und geben Sie die Anzahl der aufzubewahrenden Snapshots (Vollsicherungen) an.</p> <p>Wenn die Anzahl der vollständigen Sicherungen die angegebene Zahl überschreitet, werden die vollständigen Sicherungen, die die angegebene Zahl überschreiten, gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> |
| Vollständige Backups für eine bestimmte Anzahl von Tagen aufbewahren | Wählen Sie die Option <b>Snapshot-Kopien aufbewahren für</b> und geben Sie die Anzahl der Tage an, die Snapshots (vollständige Backups) aufbewahrt werden sollen.                                                                                                                                                                                                                                                                                                            |
| Sperrzeitraum für primäre Snapshots                                  | <p>Wählen Sie <b>Sperrzeitraum für primäre Snapshot-Kopie</b> und wählen Sie Tage, Monate oder Jahre aus.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p>                                                                                                                                                                                                                                                                              |

| Für dieses Feld...                    | Machen Sie Folgendes...                                                                                  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------|
| Sperrzeitraum für sekundäre Snapshots | Wählen Sie <b>Sperrzeitraum für sekundäre Snapshot-Kopie</b> und wählen Sie Tage, Monate oder Jahre aus. |

Wenn Sie auf einem Host in einer DAG-Konfiguration eine Datenbank mit nur Protokollsicherungen und ohne vollständige Sicherungen haben, werden die Protokollsicherungen auf folgende Weise aufbewahrt:

- Standardmäßig sucht SnapCenter die älteste vollständige Sicherung für diese Datenbank auf allen anderen Hosts im DAG und löscht alle Protokollsicherungen auf diesem Host, die vor der vollständigen Sicherung erstellt wurden.
- Sie können das oben genannte Standardaufbewahrungsverhalten für eine Datenbank auf einem Host in einem DAG mit ausschließlich Protokollsicherungen überschreiben, indem Sie den Schlüssel **MaxLogBackupOnlyCountWithoutFullBackup** in der Datei *C:\Program Files\NetApp\SnapCenter\WebApp\web.config* hinzufügen.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

Im Beispiel bedeutet der Wert 10, dass Sie bis zu 10 Protokollsicherungen auf dem Host aufbewahren.

7. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Sicherungsvorgang ausgeführt werden soll.

- Zu den Prescript-Sicherungsargumenten gehören „\$Database“ und „\$ServerInstance“.
- Zu den Postscript-Sicherungsargumenten gehören „\$Database“, „\$ServerInstance“, „\$BackupName“, „\$LogDirectory“ und „\$LogSnapshot“.

Sie können ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

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

## Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Exchange-Server hinzu

Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzauftrags, den Sie ausführen möchten, und den Schutzzeitplan zu definieren.

### Informationen zu diesem Vorgang

- Der SCRIPTS\_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- 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.
- Das Hinzufügen neuer Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken 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. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Microsoft Exchange Server-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Ansicht“ die Option „Datenbank“ aus.



Wenn Sie SnapCenter kürzlich eine Ressource hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie auf **Neue Ressourcengruppe**.
4. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name               | <div>Geben Sie den Namen der Ressourcengruppe ein.</div> <div> Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</div>                                                                  |
| Schlagwörter       | <div>Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.</div> <div>Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.</div> |



| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | <p>Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein.</p> <p>Beispiel:<br/> <code>customtext_resourcegroup_policy_hostname</code> oder <code>resourcegroup_hostname</code>. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p> |

5. Führen Sie auf der Seite „Ressourcen“ die folgenden Schritte aus:

- a. Wählen Sie den Ressourcentyp und die Datenbankverfügbarkeitsgruppe aus Dropdown-Listen aus, um die Liste der verfügbaren Ressourcen zu filtern.



Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

In den Abschnitten „Verfügbare Ressourcen“ und „Ausgewählte Ressourcen“ wird der Datenbankname mit dem FQDN des Hosts angezeigt. Dieser FQDN zeigt nur an, dass die Datenbank auf diesem bestimmten Host aktiv ist und möglicherweise keine Sicherung auf diesem Host durchführt. Sie sollten aus der Serverauswahloption einen oder mehrere Sicherungsserver auswählen, auf denen Sie eine Sicherung durchführen möchten, falls Sie in der Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben.

- b. Geben Sie den Namen der Ressource in das Suchtextfeld ein oder scrollen Sie, um eine Ressource zu finden.
- c. Um Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben, führen Sie einen der folgenden Schritte aus:
  - Wählen Sie **Alle Ressourcen auf demselben Speichervolume automatisch auswählen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
  - Wählen Sie die Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.

Ressourcengruppen von SnapCenter für Microsoft Exchange Server können nicht mehr als 30 Datenbanken pro Snapshot haben. Wenn in einer Ressourcengruppe mehr als 30 Datenbanken vorhanden sind, wird für die zusätzlichen Datenbanken ein zweiter Snapshot erstellt. Daher werden unter dem Hauptsicherungsjob zwei Unterjobs erstellt. Bei Sicherungen mit sekundärer Replikation kann es während der Ausführung einer SnapMirror oder SnapVault -Aktualisierung zu Szenarien kommen, in denen sich die Aktualisierung für beide Unteraufträge überschneidet. Der Hauptsicherungsauftrag wird für immer weiter ausgeführt, auch wenn die Protokolle anzeigen, dass der Auftrag abgeschlossen ist.

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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



Wenn eine Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** enthält, wird eine Serverauswahloption angezeigt, um einen oder mehrere Server auszuwählen. Die Serverauswahloption listet nur den Server auf, auf dem sich die ausgewählte Datenbank im NetApp -Speicher befindet.

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

- b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf  \* **in der Spalte \*Zeitpläne konfigurieren** für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **OK**.

Sie müssen dies für jede in der Richtlinie aufgeführte Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte **Angewandte Zeitpläne** im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

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

7. 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 angeben haben. `Set-SmSmtServer` .

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"](#) .

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für Exchange Server

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern und Wiederherstellen verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen

ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

## Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mithilfe des `Open-SmConnection` Cmdlet.

Dieses Beispiel öffnet eine PowerShell-Sitzung:

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie eine neue Verbindung zum Speichersystem, indem Sie das `Add-SmStorageConnection` Cmdlet.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

```
PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https  
-Timeout 60
```

3. Erstellen Sie ein neues Ausführen-als-Konto mithilfe des `Add-Credential` Cmdlet.

In diesem Beispiel wird ein neues „Ausführen als“-Konto mit dem Namen „ExchangeAdmin“ und Windows-Anmeldeinformationen erstellt:

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows  
-Credential sddev\administrator
```

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"](#) .

## Sichern Sie Exchange-Datenbanken

Wenn eine Datenbank nicht Teil einer Ressourcengruppe ist, können Sie die Datenbank oder die Datenbankverfügbarkeitsgruppe auf der Seite „Ressourcen“ sichern.

### Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten SVM zugewiesen haben.

- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn Sie eine Sicherung einer Datenbank oder einer Datenbankverfügbarkeitsgruppe durchführen möchten, die über eine aktive/passive Datenbankkopie auf einem NetApp und Nicht- NetApp -Speicher verfügt, und Sie in der Richtlinie die Option **Aktive Kopien sichern** oder **Kopien auf Servern sichern, die während der Erstellungszeit des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben, wechseln die Sicherungsaufträge in den Warnzustand. Die Sicherung ist für die aktive/passive Datenbankkopie auf NetApp -Speicher erfolgreich, für die aktive/passive Datenbankkopie auf Nicht-NetApp -Speicher schlägt die Sicherung fehl.

**Best Practice:** Führen Sie nicht gleichzeitig Backups von aktiven und passiven Datenbanken durch. Es kann zu einem Race Condition kommen und eine der Sicherungen kann fehlschlagen.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das **Microsoft Exchange Server-Plug-In** aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder „Datenbank“ oder „Datenbankverfügbarkeitsgruppe“ aus der Liste „Anzeigen“ aus.

Auf der Seite „Ressourcen“ wird  Das Symbol zeigt an, dass sich die Datenbank auf einem Nicht-NetApp -Speicher befindet.



Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und mindestens eine passive Datenbankkopie auf einem NetApp -Speicher liegt, können Sie die Datenbank schützen.

Klicken Sie auf  \* und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern. Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

- Wenn Sie eine Datenbank sichern möchten, klicken Sie auf den Datenbanknamen.
    - i. Wenn die Topologieansicht angezeigt wird, klicken Sie auf **Schützen**.
    - ii. Wenn der Assistent „Datenbank – Ressource schützen“ angezeigt wird, fahren Sie mit Schritt 3 fort.
  - Wenn Sie eine Datenbankverfügbarkeitsgruppe sichern möchten, klicken Sie auf den Namen der Datenbankverfügbarkeitsgruppe.
3. Wenn Sie einen benutzerdefinierten Snapshot-Namen angeben möchten, aktivieren Sie auf der Seite „Ressourcen“ das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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



Wenn eine Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** enthält, wird eine Serverauswahloption angezeigt, um einen oder mehrere Server auszuwählen. Die Serverauswahloption listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf einem NetApp -Speicher befindet.

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

- b.

Klicken Sie auf \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen

Zeitplan konfigurieren möchten.

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

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

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

5. 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 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 „Set-SmSmtServer“ angegeben haben.

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

Die Seite „Datenbanktopologie“ wird angezeigt.

7. Klicken Sie auf **Jetzt sichern**.

8. 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**.

9. Überwachen Sie den Fortschritt der Sicherung, indem Sie im Aktivitätsbereich unten auf der Seite auf den Auftrag doppelklicken, um die Seite mit den Auftragsdetails anzuzeigen.

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl.

Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript startet der Befehl `do_start method` den SnapCenter VMware-Plug-in-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

## 2. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit einem vollständigen Backup und einem Protokoll-Backup vom Exchange-Sicherungstyp erstellt:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit einem stündlichen vollständigen Backup und einem Protokoll-Backup vom Exchange-Sicherungstyp erstellt:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly  
-RetentionSettings  
&{'BackupType'='DATA'; 'ScheduleType'='Hourly'; 'RetentionCount'='10'}
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie erstellt, um nur Exchange-Protokolle zu sichern:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup  
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

## 3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „Get-SmResources“.

Dieses Beispiel ermittelt die Ressourcen für das Microsoft Exchange Server-Plug-In auf dem angegebenen Host:

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCE
```

## 4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

In diesem Beispiel wird eine neue Exchange Server-Datenbanksicherungsressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

In diesem Beispiel wird eine neue Backup-Ressourcengruppe für die Exchange Database Availability Group (DAG) mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

#### 5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

In diesem Beispiel wird eine neue Sicherung auf einem sekundären Speicher erstellt:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

#### 6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

In diesem Beispiel wird ein Job-Zusammenfassungsbericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

In diesem Beispiel wird ein Auftragszusammenfassungsbericht für eine bestimmte Auftrags-ID angezeigt:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie



durch Ausführen von *Get-Help command\_name*. Alternativ siehe ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

## Sichern von Exchange-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG und die Ressourcengruppe kann entweder einen ganzen DAG oder einzelne Datenbanken umfassen. Sie können die Ressourcengruppen von der Seite „Ressourcen“ aus sichern.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet beginnt. Sie sollten den Wert von konfigurieren `MaxRetryForUninitializedHosts` In `web.config` mithilfe der `Set-SmConfigSettings` PowerShell-Cmdlet.
- Wenn Sie in einer Ressourcengruppe eine Datenbank oder Datenbankverfügbarkeitsgruppe einschließen, die über eine aktive/passive Datenbankkopie auf einem NetApp und Nicht- NetApp -Speicher verfügt, und Sie in der Richtlinie die Option **Aktive Kopien sichern** oder **Kopien auf Servern sichern, die während der Erstellungszeit des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben, wechseln die Sicherungsaufträge in den Warnzustand.

Die Sicherung ist für die aktive/passive Datenbankkopie auf NetApp -Speicher erfolgreich, für die aktive/passive Datenbankkopie auf Nicht- NetApp -Speicher schlägt die Sicherung fehl.

### Informationen zu diesem Vorgang

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das **Microsoft Exchange Server-Plug-In** aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf \* klicken.  \* und wählen Sie dann das Tag aus. Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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**.
5. Überwachen Sie den Fortschritt der Sicherung, indem Sie im Aktivitätsbereich unten auf der Seite auf den Auftrag doppelklicken, um die Seite mit den Auftragsdetails anzuzeigen.

## Überwachen von Sicherungsvorgängen

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 Vorgängen 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.

## Abbrechen von Sicherungsvorgängen für die Exchange-Datenbank

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                               |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b> .<br>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b> .                                                                                                                                                                      |
| Aktivitätsbereich | a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf *  * im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.<br>b. Wählen Sie den Vorgang aus.<br>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b> . |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“

Wenn Sie die Sicherung einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen auf dem primären und sekundären Speicher anzuzeigen.

### Informationen zu diesem Vorgang

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

Sie können das folgende Symbol in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die Sicherungen auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).

-  zeigt die Anzahl der Sicherungen an, die auf dem primären Speicher verfügbar sind.
-  zeigt die Anzahl der Sicherungen an, die mithilfe der SnapMirror -Technologie auf dem sekundären Speicher gespiegelt werden.
-  zeigt die Anzahl der Sicherungen 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.

**Best Practice:** Um sicherzustellen, dass die richtige Anzahl replizierter Sicherungen angezeigt wird, empfehlen wir Ihnen, die Topologie zu aktualisieren.

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“ die Datenbank, die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Datenbankdetailansicht oder aus der Ressourcengruppendetailansicht aus.

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

4. Im Abschnitt „Zusammenfassungskarte“ finden Sie eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen.

Im Abschnitt „Zusammenfassungskarte“ werden die Gesamtzahl der Sicherungen und die Gesamtzahl der Protokollsicherungen 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 die Anwendungsressource auf 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 nach dem Failover 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** vom primären oder sekundären Speicher, um Details zu einem Backup anzuzeigen.

Die Details der Sicherungen werden in einem Tabellenformat angezeigt.

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



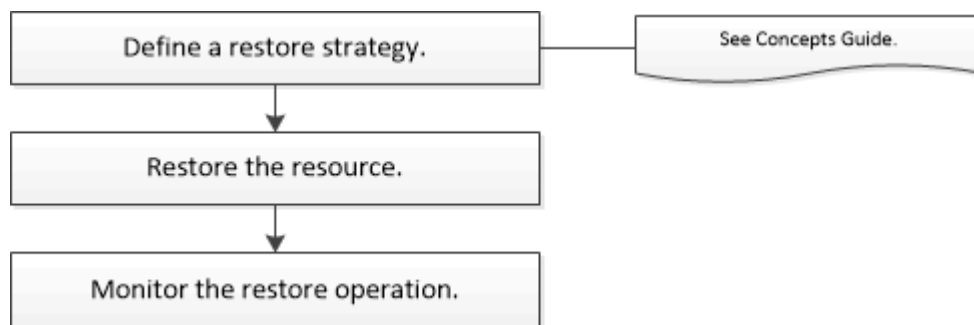
Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch löschen. Das Löschen von Snapshots wird durch die ONTAP Aufbewahrungseinstellungen geregelt.

## Wiederherstellen von Exchange-Ressourcen

### Wiederherstellungs-Workflow

Sie können SnapCenter verwenden, um Exchange-Datenbanken wiederherzustellen, indem Sie eine oder mehrere Sicherungen in Ihrem aktiven Dateisystem wiederherstellen.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Wiederherstellungsvorgänge für die Exchange-Datenbank durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripten verwenden, um Sicherungs- und Wiederherstellungsvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der Hilfe zu SnapCenter -Cmdlets oder unter ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

### Voraussetzungen für die Wiederherstellung einer Exchange-Datenbank

Bevor Sie eine Exchange Server-Datenbank aus einem SnapCenter -Plug-in für Microsoft Exchange Server-Backup wiederherstellen, müssen Sie sicherstellen, dass mehrere Anforderungen erfüllt sind.



Um die Wiederherstellungsfunktion vollständig nutzen zu können, müssen Sie sowohl den SnapCenter Server als auch das SnapCenter -Plug-in für die Exchange-Datenbank auf 4.6 aktualisieren.

- Der Exchange-Server muss online und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.

- Die Datenbanken müssen auf dem Exchange-Server vorhanden sein.



Das Wiederherstellen gelöschter Datenbanken wird nicht unterstützt.

- SnapCenter -Zeitpläne für die Datenbank müssen ausgesetzt werden.
- Der SnapCenter -Server und das SnapCenter -Plug-in für den Microsoft Exchange Server-Host müssen mit dem primären und sekundären Speicher verbunden sein, der die wiederherzustellenden Sicherungen enthält.

## Wiederherstellen von Exchange-Datenbanken

Sie können SnapCenter verwenden, um gesicherte Exchange-Datenbanken wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressourcengruppen, Datenbanken oder Datenbankverfügbarkeitsgruppen (DAGs) gesichert haben.
- Wenn die Exchange-Datenbank an einen anderen Speicherort migriert wird, funktioniert der Wiederherstellungsvorgang für alte Sicherungen nicht.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und Sie eine Wiederherstellung aus der Sicherung der passiven Datenbankkopie durchführen möchten, die sich auf einem NetApp -Speicher befindet, machen Sie die passive Kopie (NetApp -Speicher) zur aktiven Kopie, aktualisieren Sie die Ressourcen und führen Sie den Wiederherstellungsvorgang durch.

Führen Sie den `Move-ActiveMailboxDatabase` Befehl, um die passive Datenbankkopie als aktive Datenbankkopie zu erstellen.

Der "[Microsoft-Dokumentation](#)" enthält Informationen zu diesem Befehl.

### Informationen zu diesem Vorgang

- Wenn ein Wiederherstellungsvorgang für eine Datenbank ausgeführt wird, wird die Datenbank wieder auf demselben Host bereitgestellt und es wird kein neues Volume erstellt.
- Sicherungen auf DAG-Ebene müssen aus einzelnen Datenbanken wiederhergestellt werden.
- Die vollständige Datenträgerwiederherstellung wird nicht unterstützt, wenn andere Dateien als die Exchange-Datenbankdatei (.edb) vorhanden sind.

Das Plug-in für Exchange führt keine vollständige Wiederherstellung einer Festplatte durch, wenn die Festplatte Exchange-Dateien enthält, wie sie beispielsweise für die Replikation verwendet werden. Wenn eine vollständige Wiederherstellung die Exchange-Funktionalität beeinträchtigen könnte, führt das Plug-in für Exchange einen einzelnen Dateiwiederherstellungsvorgang durch.

- Das Plug-in für Exchange kann mit BitLocker verschlüsselte Laufwerke nicht wiederherstellen.
- Der `SCRIPTS_PATH` wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

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



## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich oben links auf der Ressourcenseite auf **Ressourcen**.
2. Wählen Sie das Exchange Server-Plug-In aus der Dropdown-Liste aus.
3. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Ansicht“ die Option „Datenbank“ aus.
4. Wählen Sie die Datenbank aus der Liste aus.
5. Wählen Sie in der Ansicht „Kopien verwalten“ in der Tabelle „Primäre Sicherungen“ die Option „Sicherungen“ aus und klicken Sie dann auf „\*“ .
6. Wählen Sie auf der Seite „Optionen“ eine der folgenden Protokollsicherungsoptionen aus:

| Option                          | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alle Protokollsicherungen       | Wählen Sie <b>Alle Protokollsicherungen</b> , um einen minutengenauen Sicherungswiederherstellungsvorgang durchzuführen und alle verfügbaren Protokollsicherungen nach der vollständigen Sicherung wiederherzustellen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Durch Log-Backups bis           | <p>Wählen Sie <b>Nach Protokollsicherungen bis</b>, um eine zeitpunktbezogene Wiederherstellung durchzuführen, bei der die Datenbank basierend auf Protokollsicherungen bis zum ausgewählten Protokoll wiederhergestellt wird.</p> <div><p>Die Anzahl der in der Dropdown-Liste angezeigten Protokolle basiert auf UTM. Wenn beispielsweise die vollständige Sicherungsaufbewahrung 5 und die UTM-Aufbewahrung 3 beträgt, ist die Anzahl der verfügbaren Protokollsicherungen 5, aber in der Dropdown-Liste werden nur 3 Protokolle aufgelistet, um den Wiederherstellungsvorgang durchzuführen.</p></div> |
| Nach einem bestimmten Datum bis | Wählen Sie <b>Nach bestimmtem Datum bis</b> , um das Datum und die Uhrzeit anzugeben, bis zu der Transaktionsprotokolle auf die wiederhergestellte Datenbank angewendet werden. Dieser Point-in-Time-Wiederherstellungsvorgang stellt Transaktionsprotokolleinträge wieder her, die bis zur letzten Sicherung am angegebenen Datum und zur angegebenen Uhrzeit aufgezeichnet wurden.                                                                                                                                                                                                                                                                                                          |

| Option | Beschreibung                                                                                                         |
|--------|----------------------------------------------------------------------------------------------------------------------|
| Keine  | Wählen Sie <b>Keine</b> , wenn Sie nur die vollständige Sicherung ohne Protokollsicherungen wiederherstellen müssen. |

Sie können eine der folgenden Aktionen ausführen:

- **Datenbank nach der Wiederherstellung wiederherstellen und mounten** – Diese Option ist standardmäßig ausgewählt.
- **Überprüfen Sie vor der Wiederherstellung nicht die Integrität der Transaktionsprotokolle im Backup.** – Standardmäßig überprüft SnapCenter die Integrität der Transaktionsprotokolle in einem Backup, bevor ein Wiederherstellungsvorgang durchgeführt wird.

**Best Practice:** Sie sollten diese Option nicht auswählen.

7. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Wiederherstellungsvorgang ausgeführt werden soll.

Zu den Argumenten des Wiederherstellungsvorskripts gehören \$Database und \$ServerInstance.

Zu den Postscript-Argumenten für die Wiederherstellung gehören \$Database, \$ServerInstance, \$BackupName, \$LogDirectory und \$TargetServerInstance.

Sie können ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

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.

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

10. Sie können den Status des Wiederherstellungsauftrags anzeigen, indem Sie das Aktivitätsfenster unten auf der Seite erweitern.

Sie sollten den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs** überwachen.

Wenn Sie eine aktive Datenbank aus einer Sicherung wiederherstellen, kann die passive Datenbank in den Zustand „Angehalten“ oder „Fehler“ wechseln, wenn zwischen dem Replikat und der aktiven Datenbank eine Verzögerung auftritt.

Die Statusänderung kann auftreten, wenn sich die Protokollkette der aktiven Datenbank verzweigt und einen neuen Zweig beginnt, der die Replikation unterbricht. Exchange Server versucht, das Replikat zu reparieren. Wenn dies jedoch nicht gelingt, sollten Sie nach der Wiederherstellung eine neue Sicherung erstellen und dann das Replikat erneut initialisieren.

#### PowerShell-Cmdlets

## Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer mithilfe der `Open-SmConnection Cmdlet`.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. Rufen Sie die Informationen zu den Backups ab, die Sie wiederherstellen möchten, indem Sie die `Get-SmBackup Cmdlet`.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId             | BackupName                    |
|----------------------|-------------------------------|
| BackupTime           | BackupType                    |
| -----                | -----                         |
| -----                | -----                         |
| 341                  | ResourceGroup_36304978_UTM... |
| 12/8/2017 4:13:24 PM | Full Backup                   |
| 342                  | ResourceGroup_36304978_UTM... |
| 12/8/2017 4:16:23 PM | Full Backup                   |
| 355                  | ResourceGroup_06140588_UTM... |
| 12/8/2017 6:32:36 PM | Log Backup                    |
| 356                  | ResourceGroup_06140588_UTM... |
| 12/8/2017 6:36:20 PM | Full Backup                   |

3. Stellen Sie Daten aus der Sicherung wieder her, indem Sie das `Restore-SmBackup Cmdlet`.

In diesem Beispiel wird eine aktuelle Sicherung wiederhergestellt:

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-  
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341  
-IsRecoverMount:$true
```

In diesem Beispiel wird eine zeitpunktbezogene Sicherung wiederhergestellt:

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-  
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341  
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

In diesem Beispiel wird eine Sicherung auf dem sekundären Speicher im primären Speicher wiederhergestellt:

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BuildId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

Der `-archive` Mit dem Parameter „`exe`“ können Sie die primären und sekundären Volumes angeben, die Sie für die Wiederherstellung verwenden möchten.

Der `-IsRecoverMount:$true` Mit dem Parameter können Sie die Datenbank nach der Wiederherstellung mounten.

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"](#) .

## Granulare Wiederherstellung von E-Mails und Postfächern

Mit der Single Mailbox Recovery (SMBR)-Software können Sie E-Mails oder Postfächer anstelle der gesamten Exchange-Datenbank wiederherstellen.

Das Wiederherstellen einer kompletten Datenbank, nur um eine einzelne E-Mail wiederherzustellen, kostet viel Zeit und Ressourcen. SMBR hilft bei der schnellen Wiederherstellung der E-Mails, indem es eine Klonkopie des Snapshots erstellt und dann Microsoft-APIs verwendet, um das Postfach in SMBR zu mounten. Informationen zur Verwendung von SMBR finden Sie unter ["SMBR-Administrationshandbuch"](#) .

Weitere Informationen zu SMBR finden Sie hier:

- ["So stellen Sie ein einzelnes Element manuell mit SMBR wieder her \(gilt auch für Ontrack Power Control-Wiederherstellungen\)"](#)
- ["So stellen Sie mit SnapCenter vom sekundären Speicher in SMBR wieder her"](#)
- ["Wiederherstellen von Microsoft Exchange-E-Mails aus SnapVault mithilfe von SMBR"](#)

## Wiederherstellen einer Exchange Server-Datenbank aus einem sekundären Speicher

Sie können eine gesicherte Exchange Server-Datenbank aus einem sekundären Speicher (Spiegel oder Tresor) wiederherstellen.

Sie müssen die Snapshots vom primären Speicher auf einen sekundären Speicher repliziert haben.

### Informationen zu diesem Vorgang

- 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.
- 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 **Microsoft Exchange Server-Plug-In** aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdownliste „Anzeigen“ die Option „Datenbank“ oder „Ressourcengruppe“ aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus.

Die Seite mit der Datenbank- oder Ressourcengruppentopologie wird angezeigt.

4. Wählen Sie im Abschnitt „Kopien verwalten“ **Backups** aus dem sekundären Speichersystem (Spiegel oder Tresor) aus.
5. Wählen Sie das Backup aus der Liste aus und klicken Sie dann auf  .
6. Wählen Sie auf der Seite „Speicherort“ das Zielvolume für die Wiederherstellung der ausgewählten Ressource aus.
7. Schließen Sie den Wiederherstellungsassistenten ab, überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

## Reseed einer passiven Exchange-Knotenreplik

Wenn Sie eine Replikatkopie neu initialisieren müssen, beispielsweise wenn eine Kopie beschädigt ist, können Sie mithilfe der Reseed-Funktion in SnapCenter ein Reseed auf die neueste Sicherung durchführen.

### Bevor Sie beginnen

Sie müssen eine Sicherungskopie der Datenbank erstellt haben, die Sie neu befüllen möchten.

+ Um Verzögerungen zwischen Knoten zu vermeiden, können Sie entweder vor der Durchführung eines Reseed-Vorgangs ein neues Backup erstellen oder den Host mit dem neuesten Backup auswählen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **Microsoft Exchange Server-Plug-In** aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ die entsprechende Option aus der Liste „Anzeigen“ aus:

| Option                                                                | Beschreibung                                                                  |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------|
| So führen Sie ein erneutes Seeding für eine einzelne Datenbank durch  | Wählen Sie <b>Datenbank</b> aus der Ansichtsliste.                            |
| So führen Sie ein erneutes Seeding von Datenbanken in einer DAG durch | Wählen Sie <b>Datenbankverfügbarkeitsgruppe</b> aus der Liste „Anzeigen“ aus. |

3. Wählen Sie die Ressource aus, die Sie neu säen möchten.
4. Klicken Sie auf der Seite „Kopien verwalten“ auf **Neu säen**.
5. Wählen Sie im Reseed-Assistenten aus der Liste der fehlerhaften Datenbankkopien diejenige aus, für die Sie ein Reseed durchführen möchten, und klicken Sie dann auf **Weiter**.
6. Wählen Sie im Host-Fenster den Host mit dem Backup aus, von dem Sie ein Reseed durchführen möchten, und klicken Sie dann auf **Weiter**.

7. 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.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
9. Sie können den Status des Auftrags anzeigen, indem Sie das Aktivitätsfenster unten auf der Seite erweitern.



Der Reseed-Vorgang wird nicht unterstützt, wenn sich die passive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet.

## Führen Sie mithilfe von PowerShell-Cmdlets für die Exchange-Datenbank ein erneutes Seeding eines Replikats durch

Sie können PowerShell-Cmdlets verwenden, um ein fehlerhaftes Replikat wiederherzustellen, indem Sie entweder die neueste Kopie auf demselben Host oder die neueste Kopie von einem anderen Host verwenden.

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. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer mithilfe der *Open-SmConnection* Cmdlet.

```
Open-smconnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Führen Sie ein erneutes Seeding der Datenbank durch, indem Sie *reseed-SmDagReplicaCopy* Cmdlet.

In diesem Beispiel wird die fehlgeschlagene Kopie der Datenbank mit dem Namen „execdb“ auf dem Host „mva-rx200.netapp.com“ mithilfe der neuesten Sicherung auf diesem Host neu gestartet.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb
```

In diesem Beispiel wird für die fehlgeschlagene Kopie der Datenbank mit dem Namen „execdb“ ein neues Seeding durchgeführt. Dabei wird die neueste Sicherung der Datenbank (Produktion/Kopie) auf einem alternativen Host „mva-rx201.netapp.com“ verwendet.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb -BackupHost "mva-rx201.netapp.com"
```

## Überwachen von Wiederherstellungsvorgängen

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.

## Abbrechen von Wiederherstellungsvorgängen für die Exchange-Datenbank

Sie können in der Warteschlange befindliche Wiederherstellungsaufträge abbrechen.

Sie sollten als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

### Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Wiederherstellungsvorgang entweder auf der Seite

**Überwachen** oder im Bereich **Aktivität** abbrechen.

- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

## Schritt

Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"><li>1. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li><li>2. Wählen Sie den Auftrag aus und klicken Sie auf <b>Auftrag abbrechen</b>.</li></ol>                                                                                                                                                                                     |
| Aktivitätsbereich | <ol style="list-style-type: none"><li>1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf  im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li><li>2. Wählen Sie den Vorgang aus.</li><li>3. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li></ol> |



# Schützen Sie IBM Db2

## SnapCenter Plug-in für IBM Db2

### Übersicht über das SnapCenter -Plug-in für IBM Db2

Das SnapCenter Plug-in für IBM Db2-Datenbanken ist eine hostseitige Komponente der NetApp SnapCenter software , die eine anwendungsbewusste Datenschutzverwaltung von IBM Db2-Datenbanken ermöglicht. Das Plug-in für IBM Db2-Datenbanken automatisiert die Sicherung, Wiederherstellung und das Klonen von IBM Db2-Datenbanken in Ihrer SnapCenter Umgebung.

- SnapCenter 6.0 unterstützt IBM Db2 10.5 und höher.
- SnapCenter 6.0.1 unterstützt IBM Db2 9.7.x und höher. Ab SnapCenter 6.0.1 wird außerdem IBM Db2 auf AIX unterstützt.

SnapCenter unterstützt Db2-Setups mit einer oder mehreren Instanzen. Sie können das Plug-in für die IBM Db2-Datenbank sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird Db2 als manuelle Ressource unterstützt.



Db2 pureScale-Umgebungen und Db2 Multi Node (DPF)-Systeme werden nicht unterstützt.

Wenn das Plug-in für die IBM Db2-Datenbank installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen. Sie können das Plug-in auch mit der NetApp SnapVault -Technologie verwenden, um eine Disk-to-Disk-Backup-Replikation zur Einhaltung von Standards durchzuführen.

Das SnapCenter -Plug-in für Db2 unterstützt NFS und SAN auf ONTAP und Azure NetApp Dateispeicherlayouts.

Das virtuelle Speicherlayout VMDK, vVol und RDM wird unterstützt.

### Was Sie mit dem SnapCenter Plug-in für IBM Db2 tun können

Wenn Sie das Plug-in für IBM Db2-Datenbanken in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von IBM Db2-Datenbanken und deren Ressourcen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Datenbanken hinzufügen.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

## SnapCenter Plug-in für IBM Db2-Funktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit dem Plug-in für die IBM Db2-Datenbank zu arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter .

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Kopiertechnologie**

SnapCenter verwendet die Snapshot-Technologie von NetApp mit dem Plug-in für die IBM Db2-Datenbank, um Ressourcen zu sichern.

Die Verwendung des Plug-ins für IBM Db2 bietet außerdem die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung für die Consistency Group (CG)-Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Unterstützung für Linux LVM auf dem XFS-Dateisystem.

## Vom SnapCenter Plug-in für IBM Db2 unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen Maschinen als auch auf virtuellen Maschinen (VMs). Sie müssen die Unterstützung für

Ihren Speichertyp überprüfen, bevor Sie das SnapCenter Plug-in für IBM Db2 installieren.

| Maschine          | Speichertyp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | <ul style="list-style-type: none"><li>• FC-verbundene LUNs</li><li>• Über iSCSI verbundene LUNs</li><li>• Über NFS verbundene Volumes</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| VMware ESXi       | <ul style="list-style-type: none"><li>• RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt.</li></ul> <p>Sie können die Datei <b>LinuxConfig.pm</b> unter <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> bearbeiten, um den Wert des Parameters <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> auf 1 zu setzen und nur die HBAs erneut zu scannen, die in HBA_DRIVER_NAMES aufgeführt sind.</p> <ul style="list-style-type: none"><li>• iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind</li><li>• VMDKs auf NFS-Datenspeichern</li><li>• VMDKs auf VMFS erstellt</li><li>• NFS-Volumes, die direkt mit dem Gastsystem verbunden sind</li><li>• vVol-Datenspeicher auf NFS und SAN</li></ul> <p>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p> |

## Für das IBM Db2-Plug-In erforderliche Mindest ONTAP Berechtigungen

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN erstellen
  - LUN erstellen

- LUN löschen
- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- LUN-Igroup umbenennen
- lun igroup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN persistent-reservation clear
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören

- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle

- Netzwerkschnittstelle anzeigen
- vServer

## Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für IBM Db2

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#).

## Backup-Strategie für IBM Db2

### Definieren Sie eine Sicherungsstrategie für IBM Db2

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge verfügen Sie über die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

### Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

## Schritte

1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.
4. Entscheiden Sie, ob Sie eine auf Snapshot-Kopien basierende Richtlinie erstellen möchten, um anwendungskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
6. Bestimmen Sie die Aufbewahrungsdauer für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
7. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

## Automatische Erkennung von Ressourcen auf Linux-Hosts

Ressourcen sind IBM Db2-Datenbanken und Instanzen auf dem Linux-Host, die von SnapCenter verwaltet werden. Nach der Installation des SnapCenter -Plug-ins für IBM Db2 werden die IBM Db2-Datenbanken aller Instanzen auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.

## Unterstützte Sicherungstypen

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot-Kopien basierenden Sicherungstyp für IBM Db2-Datenbanken.

### Snapshot-Kopie-basierte Sicherung

Auf Snapshot-Kopien basierende Backups nutzen die Snapshot-Technologie von NetApp , um schreibgeschützte Online-Kopien der Volumes zu erstellen, auf denen sich die IBM Db2-Datenbanken befinden.

## So verwendet das SnapCenter Plug-in für IBM Db2 Konsistenzgruppen-Snapshots

Sie können das Plug-In verwenden, um Konsistenzgruppen-Snapshots für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes aufnehmen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe besteht aus gleichzeitigen Snapshots mehrerer Volumes und bietet konsistente Kopien einer Volumengruppe.

Sie können auch die Wartezeit angeben, die der Speichercontroller benötigt, um Snapshots konsistent zu gruppieren. Die verfügbaren Wartezeitoptionen sind **Dringend**, **Mittel** und **Entspannt**. Sie können die WAFL-Synchronisierung (Write Anywhere File Layout) auch während des konsistenten Gruppen-Snapshot-Vorgangs aktivieren oder deaktivieren. Die WAFL Synchronisierung verbessert die Leistung eines Konsistenzgruppen-Snapshots.

## So verwaltet SnapCenter die Datensicherung

SnapCenter verwaltet die Datensicherungen auf Speichersystem- und Dateisystemebene.

Die Snapshots auf dem primären oder sekundären Speicher und die entsprechenden Einträge im IBM Db2-Katalog werden basierend auf den Aufbewahrungseinstellungen gelöscht.

### Überlegungen zur Festlegung von Sicherungszeitplänen für IBM Db2

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen)

Die Sicherungshäufigkeit, bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen)

Sicherungszeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird.

### Anzahl der für IBM Db2 benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

### Sicherungsnamenskonventionen für Plug-in für IBM Db2-Datenbanken

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:



```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: customtext\_resourcegroup\_policy\_hostname oder resourcegroup\_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

## Wiederherstellungs- und Recovery-Strategie für IBM Db2

### Definieren Sie eine Wiederherstellungsstrategie für IBM Db2-Ressourcen

Sie müssen vor der Wiederherstellung Ihrer Datenbank eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.



Es wird nur die manuelle Wiederherstellung der Datenbank unterstützt.

#### Schritte

1. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für manuell hinzugefügte IBM Db2-Ressourcen
2. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für automatisch erkannte IBM Db2-Datenbanken

### Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte IBM Db2-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte IBM Db2-Ressourcen.



Sie können manuell hinzugefügte IBM Db2-Ressourcen nicht wiederherstellen.

#### Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem für die Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

### Art der unterstützten Wiederherstellungsstrategie für automatisch erkanntes IBM Db2

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit

SnapCenter erfolgreich durchführen können.

Die vollständige Ressourcenwiederherstellung ist die unterstützte Wiederherstellungsstrategie für automatisch erkannte IBM Db2-Datenbanken. Dadurch werden alle Volumes, Qtrees und LUNs einer Ressource wiederhergestellt.

### Arten von Wiederherstellungsvorgängen für automatisch erkanntes IBM Db2

Das SnapCenter -Plug-in für IBM Db2 unterstützt Single File SnapRestore und Connect-and-Copy-Wiederherstellungstypen für automatisch erkannte IBM Db2-Datenbanken.

Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das ausgewählte Backup von einem SnapMirror oder SnapVault Sekundärspeicherort stammt und die Option **Complete Resource** ausgewählt ist

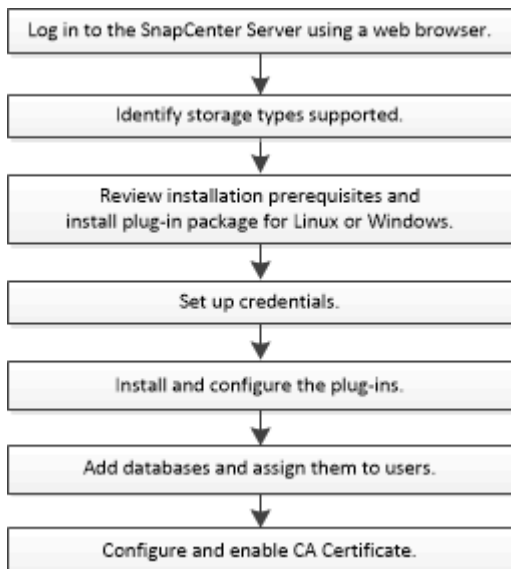
Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das Backup von einem SnapMirror oder SnapVault Sekundärspeicherort ausgewählt wird und die Option **Complete Resource** ausgewählt ist

## Vorbereiten der Installation des SnapCenter -Plug-ins für IBM Db2

### Installationsworkflow des SnapCenter Plug-ins für IBM Db2

Sie sollten das SnapCenter -Plug-in für IBM Db2 installieren und einrichten, wenn Sie IBM Db2-Datenbanken schützen möchten.



## Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows, Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. SnapCenter -Plug-in für IBM Db2 wird in Windows-, Linux- und AIX-Umgebungen unterstützt.

- Sie müssen Java 11 auf Ihrem Host installiert haben.



IBM Java wird auf Windows- und Linux-Hosts nicht unterstützt.

- Unter Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „LocalSystem“ ausgeführt werden. Dies ist das Standardverhalten, wenn das Plug-in für IBM Db2 als Domänenadministrator installiert wird.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren. Das SnapCenter -Plug-in für Microsoft Windows wird standardmäßig mit dem IBM Db2-Plug-in auf Windows-Hosts bereitgestellt.
- Der SnapCenter -Server sollte Zugriff auf den 8145- oder benutzerdefinierten Port des Plug-ins für den IBM Db2-Host haben.

### Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Während der Installation des Plug-ins für IBM Db2 auf einem Windows-Host wird das SnapCenter -Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Windows-Host installiert haben.

["JAVA für Windows herunterladen"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

### Linux- und AIX-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

["Laden Sie JAVA für Linux herunter"](#)

["Laden Sie JAVA für AIX herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Bei IBM Db2-Datenbanken, die auf einem Linux-Host ausgeführt werden, wird bei der Installation des Plug-ins für IBM Db2 automatisch das SnapCenter Plug-in für UNIX installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

## Ergänzende Befehle

Um einen zusätzlichen Befehl auf dem SnapCenter -Plug-in für IBM Db2 auszuführen, müssen Sie ihn in die Datei *allowed\_commands.config* aufnehmen.

- Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*

Um zusätzliche Befehle auf dem Plug-In-Host zuzulassen, öffnen Sie die Datei *allowed\_commands.config* in einem Editor. Geben Sie jeden Befehl in einer separaten Zeile ein. Bei den Befehlen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen (") einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: mount

Befehl: umount

Befehl: "C:\Programme\ NetApp\SnapCreator commands\sdcli.exe"

Befehl: myscript.bat

Wenn die Datei *allowed\_commands.config* nicht vorhanden ist, werden die Befehle oder die Skriptausführung blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."

Wenn der Befehl oder das Skript nicht in der Datei „*allowed\_commands.config*“ vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."



Um alle Befehle zuzulassen, sollten Sie keinen Platzhaltereintrag (\*) verwenden.

## Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host

SnapCenter ermöglicht einem Nicht-Root-Benutzer, das SnapCenter -Plug-In-Paket für Linux zu installieren und den Plug-In-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

### Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei */etc/ssh/sshd\_config*, um die Algorithmen für den

Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- /home/*LINUX\_USER*/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/bin/spl

## Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „/`<crs_home>`/bin/olsnodes“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`LINUX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host

SnapCenter 4.4 und höher ermöglicht es einem Nicht-Root-Benutzer, das SnapCenter Plug-ins-Paket für AIX zu installieren und den Plug-in-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

### Was Sie brauchen

- Sudo Version 1.8.7 oder höher.

- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/bin/spl`

## Schritte

1. Melden Sie sich beim AIX-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für AIX installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei `/etc/sudoers` hinzu.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „`/<crs_home>/bin/olsnodes`“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`AIX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den Prüfsummenwert aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.



| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                                                                                                                                                                        |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>5 GB</p> <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java und OpenJDK</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                |

## Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux

Bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren, sollten Sie mit einigen grundlegenden Anforderungen an Speicherplatz und Größe des Hostsystems vertraut sein.

| Artikel         | Anforderungen                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <div>2 GB</div> <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | <p>Java 11 Oracle Java und OpenJDK</p> <p>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.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                  |

## Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für IBM Db2

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Datenbanken oder Windows-Dateisystemen erstellen.

### Informationen zu diesem Vorgang

- Linux-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldeinformationen für den Root-Benutzer oder für einen Nicht-Root-Benutzer mit Sudo-Berechtigungen einrichten, um den Plug-In-Prozess zu installieren und zu starten.

**Best Practice:** Obwohl Sie Anmeldeinformationen für Linux erstellen dürfen, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

- Windows-Hosts

Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.

Sie müssen die Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die zum Konfigurieren der Anmeldeinformationen erforderlichen Informationen an:

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |

| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername                      | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i></p> <p>Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (&lt;) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als &lt;!10, kleiner als 10 &lt;!, Backtick `12.</p> |
| Passwort                          | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Authentifizierungsmodus           | Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen <b>Sudo-Berechtigungen verwenden</b>, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p> <div data-bbox="873 1839 927 1892">  </div> <p>Gilt nur für Linux-Benutzer.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

## Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

### Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -Effectivelmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$  
.. Fügen Sie der Gruppe Computerobjekte hinzu.  
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des Dienstkontos.
```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:

- a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                |
|---------|----------------|-----------|-----------------------------------------------|
| -----   | -----          | -----     | -----                                         |
| True    | No             | Success   | {Active Directory Domain Services, Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- Starten Sie Ihren Host neu.
  - Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
  - Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
- Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
  - Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Installieren Sie das SnapCenter -Plug-in für IBM Db2

### Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren.

#### Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zur Verwaltung von Hosts.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

["Konfigurieren Sie das gruppenverwaltete Dienstkonto unter Windows Server 2016 oder höher für IBM Db2"](#)

### Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.

### 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            | <p>Wählen Sie den Hosttyp aus:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> </ul> <div>  <p>Das Plug-in für IBM Db2 wird auf dem IBM Db2-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> </div> |
| Hostname           | <p>Geben Sie den Hostnamen für die Kommunikation ein. Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p>                                                                                                 |

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationen | <p>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.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div>  <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

Wenn Sie die REST-API zum Installieren des Plug-ins für Db2 verwenden, müssen Sie die Version als 3.0 übergeben. Beispiel: Db2:3.0

6. (Optional) Klicken Sie auf **Weitere Optionen**.

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen              | <p>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.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |



| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installationspfad                                                                           | <p>Das Plug-in für IBM Db2 wird auf dem IBM Db2-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> <ul style="list-style-type: none"> <li>Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter. Optional können Sie den Pfad anpassen.</li> <li>Für das SnapCenter Plug-ins-Paket für Linux ist der Standardpfad /opt/ NetApp/snapcenter. Optional können Sie den Pfad anpassen.</li> </ul>                                                                                  |
| Vorinstallationsprüfungen überspringen                                                      | 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.                                                                                                                                                                                                                                                                                                                                                                    |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | <p>Aktivieren Sie für Windows-Hosts dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.</p> <div>  <p>Geben Sie den gMSA-Namen im folgenden Format an:<br/>Domänenname\Kontoname\$.</p> </div> <div>  <p>gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.</p> </div> |

7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-Ins) und Java 11 (für Windows- und Linux-Plug-Ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, 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, müssen Sie das Problem beheben.



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

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



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

#### 9. Überwachen Sie den Installationsfortschritt.

- Für Windows-Plug-Ins befinden sich die Installations- und Upgrade-Protokolle unter: `C:\Windows\SnapCenter plugin\Install<JOBID>\`
- Für Linux-Plug-Ins befinden sich die Installationsprotokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log` und die Upgrade-Protokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log`

#### Nach Abschluss

Wenn Sie auf SnapCenter 6.0 oder höher aktualisieren möchten, wird das vorhandene PERL-basierte Plug-in für Db2 vom Remote-Plug-in-Server deinstalliert.

#### Installieren Sie SnapCenter Plug-in-Pakete für Linux oder Windows auf mehreren Remote-Hosts mithilfe von Cmdlets

Sie können die SnapCenter -Plug-in-Pakete für Linux oder Windows mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

#### Bevor Sie beginnen

Sie müssen sich auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

#### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-In auf mehreren Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

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](#) .

Sie können die Option `-skippercheck` verwenden, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

#### Installieren Sie das SnapCenter -Plug-in für IBM Db2 auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle

Sie sollten das SnapCenter Plug-in für die IBM Db2-Datenbank mithilfe der SnapCenter -Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie das Plug-In für die IBM Db2-Datenbank entweder im Konsolenmodus oder im Hintergrundmodus

mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

### Bevor Sie beginnen

- Sie sollten das Plug-in für die IBM Db2-Datenbank auf jedem Linux-Host installieren, auf dem sich der IBM Db2-Client befindet.
- Der Linux-Host, auf dem Sie das SnapCenter -Plug-in für die IBM Db2-Datenbank installieren, muss die abhängigen Software-, Datenbank- und Betriebssystemanforderungen erfüllen.

Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den unterstützten Konfigurationen.

#### ["NetApp Interoperabilitätsmatrix-Tool"](#)

- Das SnapCenter -Plug-in für die IBM Db2-Datenbank ist Teil des SnapCenter Plug-in-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins-Paket für Linux installieren, sollten Sie SnapCenter bereits auf einem Windows-Host installiert haben.

### Informationen zu diesem Vorgang

Wenn keine Parameter angegeben sind, wird SnapCenter mit Standardwerten installiert.

### Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter Plug-ins-Pakets für Linux (snapcenter\_linux\_host\_plugin.bin) von C:\ProgramData\NetApp\ SnapCenter\Package Repository auf den Host, auf dem Sie das Plug-in für IBM Db2 installieren möchten.

Sie können auf diesen Pfad von dem Host aus zugreifen, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei kopiert haben.

3. Installieren Sie das Plug-In:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT gibt den SMCore HTTPS-Kommunikationsport an.
- -DSERVER\_IP gibt die IP-Adresse des SnapCenter -Servers an.
- -DSERVER\_HTTPS\_PORT gibt den HTTPS-Port des SnapCenter -Servers an.
- -DUSER\_INSTALL\_DIR gibt das Verzeichnis an, in dem Sie das SnapCenter Plug-Ins-Paket für Linux installieren möchten.
- DINSTALL\_LOG\_NAME gibt den Namen der Protokolldatei an.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Bearbeiten Sie die Datei /<Installationsverzeichnis>/  
NetApp/snapcenter/scc/etc/SC\_SMS\_Services.properties und fügen Sie dann den Parameter

PLUGINS\_ENABLED = DB2:3.0 hinzu.

5. Fügen Sie den Host mit dem Cmdlet Add-Smhost und den erforderlichen Parametern zum SnapCenter -Server hinzu.

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 ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Überwachen Sie den Status der Installation des Plug-ins für IBM Db2

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

## CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

### Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

#### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
  - a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-ChildItem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

### Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

#### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Konfigurieren Sie das CA-Zertifikat für den SnapCenter IBM Db2 Plug-Ins-Dienst auf dem Linux-Host

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

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter `/opt/NetApp/snapcenter/scc/etc` befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Dies ist der Wert, der dem Schlüssel „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_in_cert" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE\_PASS in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

#### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder  
Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

#### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```



5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.

7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE\_PASS in der Datei agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei agent.properties.

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC\_CERTIFICATE\_ALIAS.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

#### Informationen zu diesem Vorgang

- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-Ins ist „opt/NetApp/snapcenter/scc/etc/crl“.

#### Schritte

1. Sie können das Standardverzeichnis in der Datei agent.properties anhand des Schlüssels CRL\_PATH ändern und aktualisieren.

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

### Konfigurieren Sie das CA-Zertifikat für den SnapCenter IBM Db2 Plug-Ins-Dienst auf dem Windows-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-

In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter -Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-ins verwenden die Datei *keystore.jks*, die sich unter *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc* befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Es handelt sich um den Wert, der dem Schlüssel *KEYSTORE\_PASS* entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

```
C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

```
keytool -keypasswd -alias "Aliasname_im_Zertifikat" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel *KEYSTORE\_PASS* in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

#### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher `C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc`
2. Suchen Sie die Datei `keystore.jks`.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels `KEYSTORE_PASS` in der Datei `agent.properties`.

```
keytool -keypasswd -alias "Aliasname_im_CA_Zertifikat" -keystore keystore.jks
```

8. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei `agent.properties`.

Aktualisieren Sie diesen Wert anhand des Schlüssels `SCC_CERTIFICATE_ALIAS`.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter -Plug-Ins

#### Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe ["So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat"](#) .
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.

- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist 'C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\crl'.

### Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* anhand des Schlüssels 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.

## Bereiten Sie sich auf den Datenschutz vor

## Voraussetzungen für die Verwendung des SnapCenter Plug-Ins für IBM Db2

Bevor Sie das SnapCenter -Plug-in für IBM Db2 verwenden, muss der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich beim SnapCenter -Server an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen und gegebenenfalls Anmeldeinformationen erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

Sie müssen den Java-Pfad in der Umgebungspfadvariable des Hostcomputers festlegen.

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.

## So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von IBM Db2 verwendet

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei den Ressourcen handelt es sich in der Regel um IBM Db2-Datenbanken, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Sicherungshäufigkeit, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

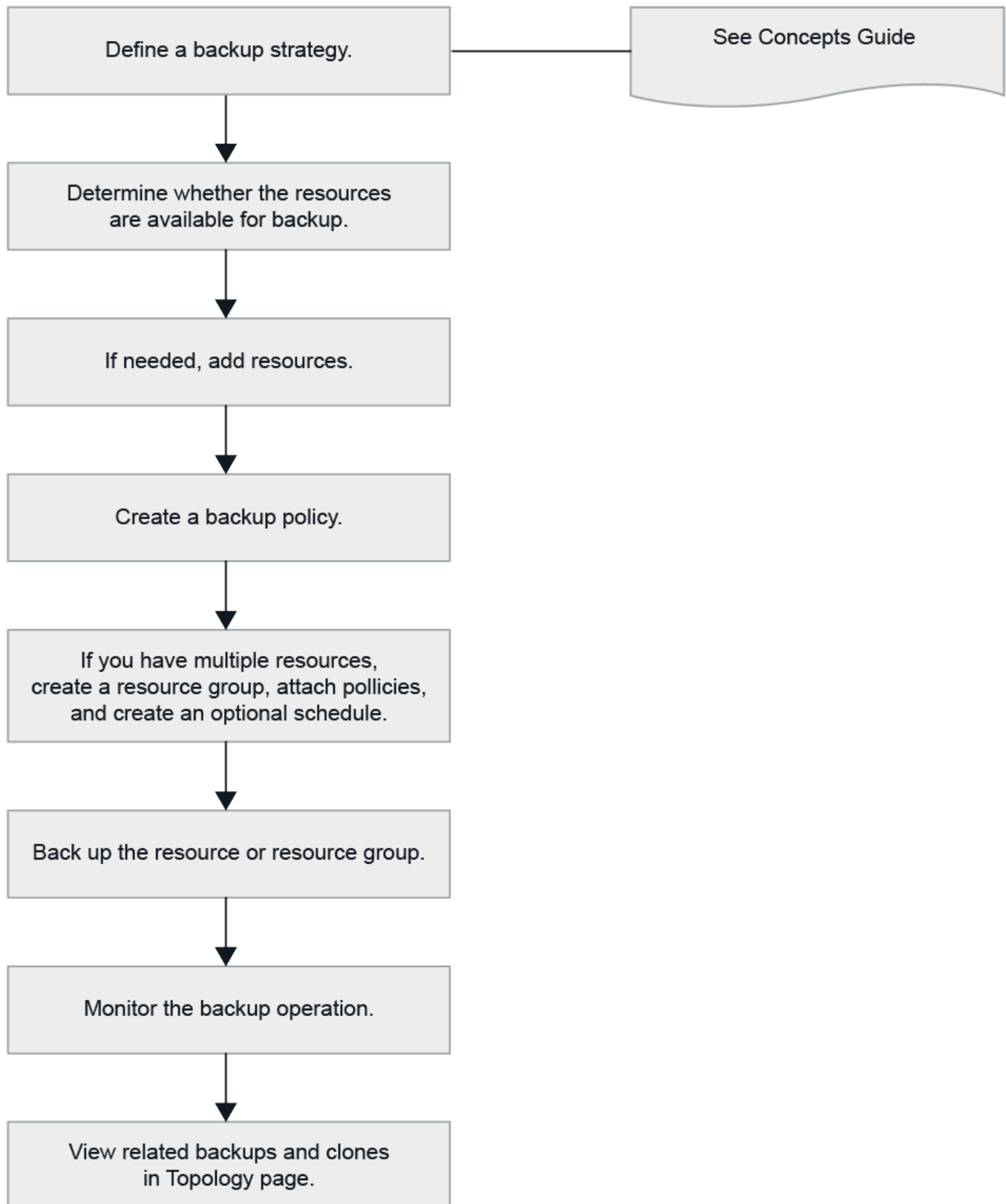
Stellen Sie sich eine Ressourcengruppe so vor, dass sie definiert, was Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als ob sie definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken im Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird.

# Sichern von IBM Db2-Ressourcen

## Sichern von IBM Db2-Ressourcen

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Sicherungsworkflow umfasst die Planung, die Identifizierung der zu sichernden Datenbanken, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets. ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

## Automatisches Erkennen der Datenbanken

Ressourcen sind IBM Db2-Datenbanken auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren IBM Db2-Datenbanken ermittelt haben.

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen abgeschlossen haben.
- Das SnapCenter Plug-in für IBM Db2 unterstützt keine automatische Erkennung der in virtuellen RDM/VMDK-Umgebungen vorhandenen Ressourcen. Sie müssen die Speicherinformationen für virtuelle Umgebungen angeben, während Sie die Datenbanken manuell hinzufügen.

### Informationen zu diesem Vorgang

- Nach der Installation des Plug-ins werden alle Datenbanken auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.
- Nur Datenbanken werden automatisch erkannt.

Die automatisch erkannten Ressourcen können nicht geändert oder gelöscht werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für IBM Db2 aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste „Anzeigen“ aus.
3. (Optional) Klicken Sie auf  \* und wählen Sie dann den Hostnamen aus.

Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen anzuzeigen.

Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp -Speichersystem befindet und geschützt ist und kein Sicherungsvorgang ausgeführt wird, wird in der Spalte „Gesamtstatus“ die Meldung „Sicherung nicht ausgeführt“ angezeigt. Andernfalls ändert sich der Status basierend auf dem letzten Sicherungsstatus in „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

## Ressourcen manuell zum Plug-In-Host hinzufügen

Die automatische Erkennung wird auf Windows-Hosts nicht unterstützt. Sie müssen Db2-Instanzen und Datenbankressourcen manuell hinzufügen.

### Bevor Sie beginnen



- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten von Speichersystemverbindungen abgeschlossen haben.

### Informationen zu diesem Vorgang

Die manuelle Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und dann das SnapCenter Plug-in für IBM Db2 aus der Dropdown-Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **IBM DB2-Ressource hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Name                 | Geben Sie den Datenbanknamen an.                                                                                                  |
| Hostname             | Geben Sie den Hostnamen ein.                                                                                                      |
| Typ                  | Wählen Sie eine Datenbank oder Instanz aus.                                                                                       |
| Beispiel             | Geben Sie den Namen der Instanz an, die der Datenbank übergeordnet ist.                                                           |
| Anmeldeinformationen | Wählen Sie die Anmeldeinformationen aus oder fügen Sie Informationen zu den Anmeldeinformationen hinzu.<br><br>Dies ist optional. |

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ einen Speichertyp und ein oder mehrere Volumes, LUNs und Qtrees aus und klicken Sie dann auf **Speichern**.

Optional: Sie können auf das \* klicken  \* Symbol zum Hinzufügen weiterer Volumes, LUNs und Qtrees aus anderen Speichersystemen.

5. Optional: Geben Sie auf der Seite „Ressourceneinstellungen“ für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für das IBM Db2-Plug-In ein.
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Die Datenbanken werden zusammen mit Informationen wie dem Hostnamen, den zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie die Ressourcen den Benutzern zuweisen. Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

["Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"](#)

Nachdem Sie die Datenbanken hinzugefügt haben, können Sie die Details der IBM Db2-Datenbank ändern.

## Erstellen von Sicherungsrichtlinien für IBM Db2

Bevor Sie SnapCenter zum Sichern von IBM Db2-Ressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren.

### Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für IBM Db2-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen von Ressourcen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

Darüber hinaus können Sie in der Richtlinie Replikations-, Skript- und Anwendungseinstellungen angeben. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

### 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. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie den Speichertyp aus.
  - b. Geben Sie im Abschnitt **Benutzerdefinierte Sicherungseinstellungen** alle spezifischen Sicherungseinstellungen an, die im Schlüssel-Wert-Format an das Plug-In übergeben werden müssen.

Sie können mehrere Schlüsselwerte angeben, die an das Plug-In übergeben werden sollen.

6. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Aktionen aus.

- a. Geben Sie die Zeitplanhäufigkeit an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber auch jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- a. Führen Sie im Abschnitt „Snapshot-Einstellungen“ die folgenden Aktionen aus:

| Wenn Sie wollen...                                                 | Dann...                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Schnappschüssen             | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> |
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | <p>Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.</p>                                                                                                               |
| Sperrzeitraum für Snapshot-Kopien                                  | <p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopien</b> und geben Sie Tage, Monate oder Jahre an.</p> <p>Die Aufbewahrungsdauer von Snaplock sollte weniger als 100 Jahre betragen.</p>                                                                                             |



Für Snapshot-Kopien-basierte Backups müssen Sie 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.

- b. Geben Sie die Richtlinienbezeichnung an.

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.

7. 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).<br><br>Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden. |
| Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben  | Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).                                                                                                          |
| Fehleranzahl der Wiederholungsversuche                                               | Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.                                                                                                                |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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

## Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### Informationen zu diesem Vorgang

- 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

- Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
- Klicken Sie auf der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
- Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | <p>Geben Sie einen Namen für die Ressourcengruppe ein.</p> <div>  <p>Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</p> </div>                                                                                                  |
| Schlagwörter                                                  | <p>Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.</p> <p>Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.</p>                                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | <p>Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.</p> <p>Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p> |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

Dies hilft, Informationen auf dem Bildschirm zu filtern.

5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                             | Machen Sie Folgendes...                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Snapshot-Vorgangs der Konsistenzgruppe zu warten | <p>Wählen Sie <b>Dringend</b>, <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs anzugeben.</p> <p>Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.</p> |

| Für dieses Feld...                  | Machen Sie Folgendes...                                                             |
|-------------------------------------|-------------------------------------------------------------------------------------|
| WAFL -Synchronisierung deaktivieren | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden. |

+

- Klicken Sie auf den Pfeil **Skripts** 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.
- Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

| Parameter            | Einstellung                | Beschreibung                                                                                                                                                     |
|----------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIV_LOG_ENABLE    | (J/N)                      | Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle.                                                                                        |
| ARCHIV_LOG_RETENTION | Anzahl_der_Tage            | Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden.<br><br>Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein. |
| ARCHIVE_LOG_DIR      | change_info_directory/logs | Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.                                                                                              |

| Parameter                     | Einstellung      | Beschreibung                                                                                                                                                                                                                                                   |
|-------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIVE_LOG_EXT               | Dateierweiterung | Gibt die Erweiterungslänge der Archivprotokolldatei an.<br><br>Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.16151855 1942 9 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (J/N)            | Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen.<br><br>Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.                                                                         |



Die benutzerdefinierten Schlüssel-Wert-Paare werden für IBM Db2 Linux-Plug-in-Systeme unterstützt, jedoch nicht für IBM Db2-Datenbanken, die als zentrales Windows-Plug-in registriert sind.

- c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                                                                        | Dann...                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar. | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.                                                                                      |
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                                                                                    | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                                                                     |
| Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot-Kopien zu erstellen.                                                                                                           | Wählen Sie <b>Andere</b> aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen. |

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

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



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

Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

- b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \*  \* für die Richtlinie, die Sie konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist „policy\_name“ 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. Der SMTP-Server muss unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für IBM Db2-Ressourcen 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                                                                         |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> .                                                        |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für IBM Db2

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern, Wiederherstellen oder Klonen von IBM Db2-Datenbanken verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

### Schritte

- Klicken Sie auf **SnapCenterPS**, um PowerShell Core zu starten.
- Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

- Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

Dieses Beispiel zeigt, wie Sie mit Windows-Anmeldeinformationen neue Anmeldeinformationen mit dem Namen „FinanceAdmin“ erstellen:

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux  
-AuthenticationType PasswordBased -Credential db2hostuser  
-EnableSudoPrivileges:$true
```

- Fügen Sie den IBM Db2-Kommunikationshost zum SnapCenter Server hinzu.

Für Linux:

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

Für Windows:

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. Installieren Sie das Paket und das SnapCenter -Plug-in für IBM Db2 auf dem Host.

Für Linux:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2
```

Für Windows:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2, SCW
```

6. Legen Sie den Pfad zur SQLLIB fest.

Für Windows verwendet das Db2-Plug-In den Standardpfad für den SQLLIB-Ordner:  
„C:\Programme\IBM\SQLLIB\BIN“.

Wenn Sie den Standardpfad überschreiben möchten, verwenden Sie den folgenden Befehl.

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
```

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](#) .

## Sichern von Db2-Datenbanken

Das Sichern einer Datenbank umfasst das Herstellen einer Verbindung mit dem SnapCenter -Server, das Hinzufügen von Ressourcen, das Hinzufügen einer Richtlinie, das Erstellen einer Sicherungsressourcengruppe und das Sichern.

**Bevor Sie beginnen**

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Stellen Sie bei Sicherungsvorgängen auf Basis von Snapshot-Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Bei Pre- und Post-Befehlen für Quiesce-, Snapshot- und Unquiesce-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Wählen  und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- Wählen Sie den Pfeil **Backups** aus, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                            | Machen Sie Folgendes...                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Vorgangs „Consistency Group Snapshot“ zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für die Fertigstellung des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                           | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

- Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.

Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

- Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                   | Dann...                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                               | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                      |
| SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.                                       |
| So geben Sie den Befehl zum Erstellen eines Snapshots ein                                                                                                | Wählen Sie <b>Andere</b> und geben Sie dann den Befehl zum Erstellen eines Snapshots ein. |

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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

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

- b. Wählen \* \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

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

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Wählen Sie **Jetzt sichern**.

10. 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. Wählen Sie **Backup**.

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

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-SmConnection
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Fügen Sie mithilfe des Cmdlets `Add-SmResources` manuelle Ressourcen hinzu.

Dieses Beispiel zeigt, wie eine IBM Db2-Instanz hinzugefügt wird:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

Für die Db2-Datenbank:



```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.
4. Schützen Sie die Ressource oder fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.
5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert wird:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

In diesem Beispiel wird eine Db2-Instanz gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
db2_policy
```

In diesem Beispiel wird eine Db2-Datenbank gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCD";"PluginName"="DB2"
} -Policy db2_policy
```

6. Überwachen Sie den Auftragsstatus (wird ausgeführt, abgeschlossen oder fehlgeschlagen) mithilfe des Cmdlets Get-smJobSummaryReport.

```
PS C:\> Get-SmJobSummaryReport -JobId 467
```

```
SmJobId           : 467
JobCreatedDateTime :
JobStartDateTime  : 27-Jun-24 01:40:09
JobEndDateTime    : 27-Jun-24 01:41:15
JobDuration       : 00:01:06.7013330
JobName           : Backup of Resource Group
                  'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
                  'snapshot-based-db2'
JobDescription     :
Status            : Completed
IsScheduled       : False
JobError          :
JobType           : Backup
PolicyName        : db2_policy
JobResultData     :
```

7. Überwachen Sie die Details des Sicherungsauftrags wie Sicherungs-ID und Sicherungsname, um mithilfe des Cmdlets Get-SmBackupReport Wiederherstellungs- oder Klonvorgänge durchzuführen.

```
PS C:\> Get-SmBackupReport -JobId 467
```

```
BackedUpObjects      : {WINCIR}
FailedObjects        : {}
IsScheduled           : False
HasMetadata           : False
SmBackupId            : 84
SmJobId               : 467
StartDateTime         : 27-Jun-24 01:40:09
EndDateTime          : 27-Jun-24 01:41:15
Duration              : 00:01:06.7013330
CreatedDateTime       : 27-Jun-24 18:39:45
Status                : Completed
ProtectionGroupName   : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId   : 23
PolicyName            : db2_policy
SmPolicyId            : 13
BackupName            : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus    : NotApplicable
VerificationStatuses  :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses    :
ReportDataCreatedDateTime :
PluginCode            : SCC
PluginName            : DB2
PluginDisplayName     : IBM DB2
JobTypeId             :
JobHost               : HOSTFQDN
```

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"](#) .

## Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

### Informationen zu diesem Vorgang

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie  und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
  - a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Überwachen von IBM Db2-Sicherungsvorgängen

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 Sie Datenschutzvorgänge für IBM Db2-Datenbanken 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.

### Abbrechen von Sicherungsvorgängen für IBM Db2

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzuberechnen.

- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

## Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ul style="list-style-type: none"> <li>a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li> <li>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b>.</li> </ul>                                                                                                                                                                         |
| Aktivitätsbereich | <ul style="list-style-type: none"> <li>a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li> <li>b. Wählen Sie den Vorgang aus.</li> <li>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li> </ul> |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## Anzeigen von IBM Db2-Sicherungen und -Klonen auf der Seite „Topologie“

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

### Informationen zu diesem Vorgang

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.

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

### 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 Ressourcengruppdetailansicht aus.

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

4. Überprüfen Sie die **Zusammenfassungskarte**, um eine Zusammenfassung der Anzahl der auf dem primären und sekundären Speicher verfügbaren Backups und Klone anzuzeigen.

Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Klone an.

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 die Anwendungsressource auf 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.

Nach der On-Demand-Sicherung werden durch Klicken auf die Schaltfläche **Aktualisieren** die Details der Sicherung oder des Klons aktualisiert.

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.

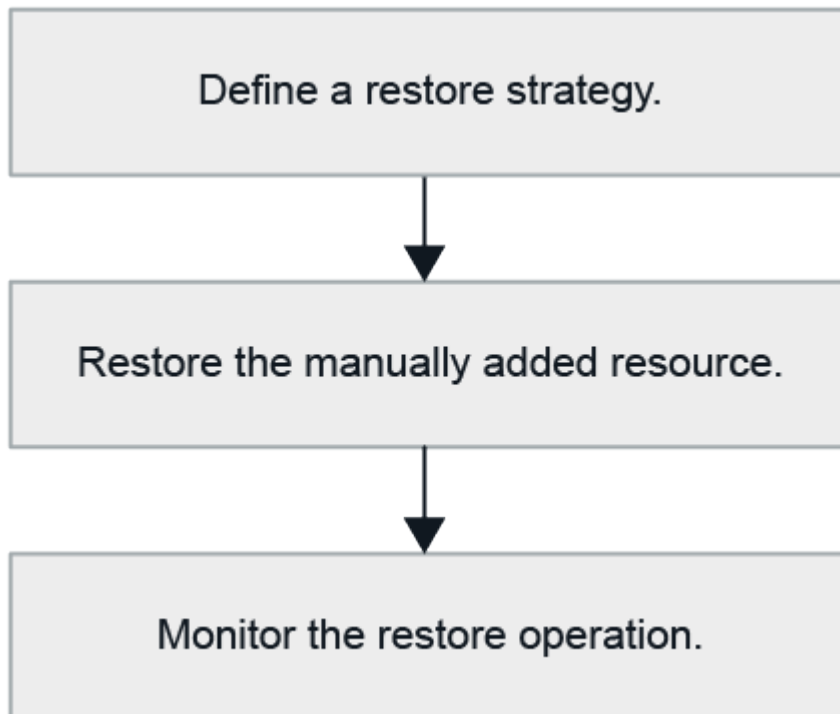
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf  .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf  .

## IBM Db2 wiederherstellen

### Wiederherstellungs-Workflow

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.



## Wiederherstellen einer manuell hinzugefügten Ressourcensicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                           |                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| search                                      |                        |
| Backup Name                                 | End Date                                                                                                  |
| rg1_scpr0191685001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option **Vollständige Ressource** aus.
  - a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumes der IBM Db2-Datenbank wiederhergestellt.

Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

Sie können mehrere LUNs auswählen.



Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, Qtrees oder LUNs wiederhergestellt.

7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
9. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

### Nach Abschluss

Eine Wiederherstellung ist nur möglich, wenn der Rollforward-Status „DB ausstehend“ lautet. Dieser Status gilt für Db2-Datenbanken mit aktivierter Archivprotokollierung.

### PowerShell-Cmdlets

#### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-SmConnection
```

2. Identifizieren Sie die Sicherung, die Sie wiederherstellen möchten, mithilfe der Cmdlets Get-SmBackup und Get-SmBackupReport.

Dieses Beispiel zeigt, dass für die Wiederherstellung zwei Sicherungen zur Verfügung stehen:

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library
```

|                | BackupId | BackupName                    | BackupTime        |
|----------------|----------|-------------------------------|-------------------|
| BackupType     |          |                               |                   |
|                | -----    | -----                         | -----             |
| -----          |          |                               |                   |
|                | 1        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:02:32 |
| AM Full Backup |          |                               |                   |
|                | 2        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:23:17 |
| AM             |          |                               |                   |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId           : 113
SmJobId              : 2032
StartDateTime        : 2/2/2015 6:57:03 AM
EndDateTime          : 2/2/2015 6:57:11 AM
Duration              : 00:00:07.3060000
CreatedDateTime       : 2/2/2015 6:57:23 AM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName            : Vault
SmPolicyId            : 18
BackupName            : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus    : NotVerified

SmBackupId           : 114
SmJobId              : 2183
StartDateTime        : 2/2/2015 1:02:41 PM
EndDateTime          : 2/2/2015 1:02:38 PM
Duration              : -00:00:03.2300000
CreatedDateTime       : 2/2/2015 1:02:53 PM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName            : Vault
SmPolicyId            : 18
BackupName            : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus    : NotVerified
```

### 3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.



AppObjectId ist „Host\Plugin\UID“, wobei UID = <Instanzname> für die manuell ermittelte DB2-Instanzressource und UID = <Instanzname>\<Datenbankname> für die IBM Db2-Datenbankressource steht. Sie können die ResourceID über das Cmdlet „Get-smResources“ abrufen.

```
Get-smResources -HostName cn24.sccore.test.com -PluginCode DB2
```

Dieses Beispiel zeigt, wie die Datenbank vom primären Speicher wiederhergestellt wird:

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

Dieses Beispiel zeigt, wie die Datenbank aus dem sekundären Speicher wiederhergestellt wird:

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>"; "Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"})
```

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"](#) .

## Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Die automatische Wiederherstellung wird nicht unterstützt.
- 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 **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.

2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                            |                                                                                                           |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| search                                       |                        |
| Backup Name                                  | End Date                                                                                                  |
| rg1_scscr0191685001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ **Vollständige Ressource** aus, um die konfigurierten Datenvolumes der IBM Db2-Datenbank wiederherzustellen.
7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Unmount-Befehle erforderlich.

8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle erforderlich.

9. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

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

### Nach Abschluss

Eine Wiederherstellung ist nur möglich, wenn der Rollforward-Status „DB ausstehend“ lautet. Dieser Status gilt für Db2-Datenbanken mit aktivierter Archivprotokollierung.

## Überwachen von IBM Db2-Wiederherstellungsvorgängen

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 von IBM Db2-Ressourcensicherungen

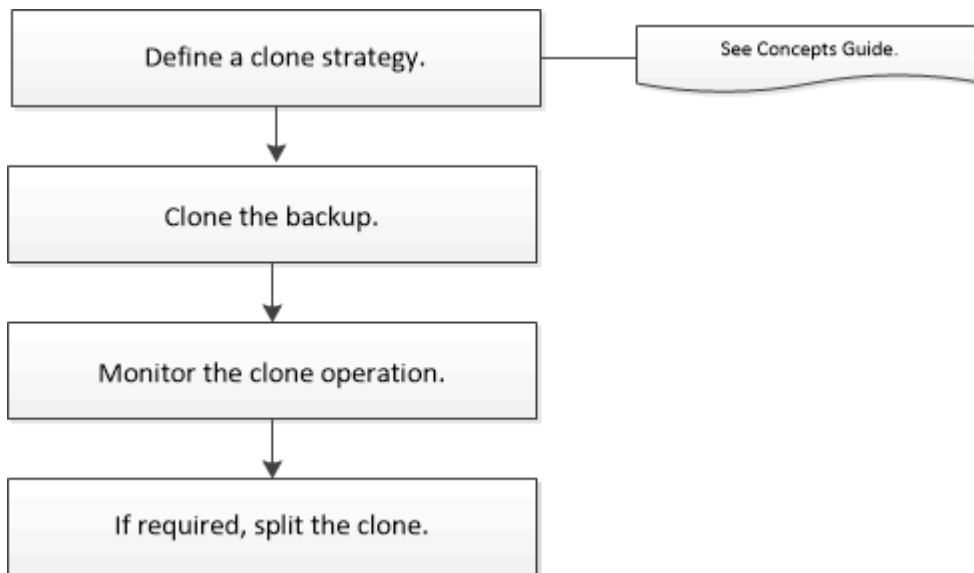
## Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

### Informationen zu diesem Vorgang

- Sie können auf dem IBM Db2-Quellserver klonen.
- Sie können Ressourcensicherungen aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Für Datenextraktions- und Manipulationstools beim Befüllen von Data Warehouses
  - So stellen Sie versehentlich gelöschte oder geänderte Daten wieder her

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

### Nach Abschluss

Nach dem Klonen der automatisch erkannten Db2-Ressourcen wird die geklonte Ressource als manuelle Ressource markiert. Klicken Sie auf **Ressourcen aktualisieren**, um die geklonte Db2-Ressource wiederherzustellen. Wenn Sie den Klon löschen, werden auch der Speicher und der Host bereinigt.

Wenn Sie die Ressourcen nach dem Klonvorgang nicht aktualisieren und versuchen, den Klon zu löschen, werden der Speicher und der Host nicht bereinigt. Sie müssen die Einträge manuell in der fstab löschen.

## Klonen einer IBM Db2-Sicherung

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen.



## Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Beim Erstellen eines Klons für Db2 auf einem alternativen Host müssen Sie für den Mountpfad des Klons eine n-1-Verzeichnisstruktur erstellen, die mit dem ursprünglichen Mountpfad auf dem anderen Host identisch ist. Der Mount-Pfad sollte über die Ausführungsberechtigung 755 verfügen.
- Bei Befehlen vor oder nach dem Klonen sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

## Informationen zu diesem Vorgang

- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume"] .
- 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:

| Für dieses Feld...                         | Machen Sie Folgendes...                                                                                                                                           |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server klonen                              | Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.                                                                                                 |
| Zielklon-Instanz                           | Geben Sie die Ziel-ID der Db2-Kloninstanz ein, die aus den vorhandenen Sicherungen geklont werden soll.<br><br>Dies gilt nur für Ressourcen des Speichertyps ANF. |
| Name des Zielklons                         | Geben Sie den Namen des Klons ein.<br><br>Dies gilt nur für Db2-Datenbankressourcen.                                                                              |
| NFS-Export-IP-Adresse                      | Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden.<br><br>Dies gilt nur für Ressourcen des NFS-Speichertyps.          |
| Max. Durchsatz des Kapazitätspools (MiB/s) | Geben Sie den maximalen Durchsatz eines Kapazitätspools ein.                                                                                                      |

7. Führen Sie auf der Seite „Skripts“ die folgenden Schritte aus:



Die Skripte werden auf dem Plug-in-Host ausgeführt.

- a. Geben Sie die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
  - Befehl vor dem Klonen: Löschen Sie vorhandene Datenbanken mit demselben Namen
  - Befehl nach dem Klonen: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.
- b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Mount-Befehl für ein Volume oder einen Qtree auf einer Linux-Maschine:

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

### Nach Abschluss

Nach dem Klonen der automatisch erkannten Db2-Ressourcen wird die geklonte Ressource als manuelle Ressource markiert. Klicken Sie auf **Ressourcen aktualisieren**, um die geklonte Db2-Ressource wiederherzustellen. Wenn Sie den Klon löschen, werden auch der Speicher und der Host bereinigt.

Wenn Sie die Ressourcen nach dem Klonvorgang nicht aktualisieren und versuchen, den Klon zu löschen, werden der Speicher und der Host nicht bereinigt. Sie müssen die Einträge manuell in der fstab löschen.

### PowerShell-Cmdlets

#### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Sicherungen auf, die mit dem Cmdlet Get-SmBackup oder Get-SmResourceGroup geklont werden können.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
C:\PS>PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime              | BackupType  |
|----------|-------------------------------|-------------------------|-------------|
| -----    | -----                         | -----                   | -----       |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015<br>11:02:32 AM | Full Backup |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015<br>11:23:17 AM |             |

In diesem Beispiel werden Informationen zu einer angegebenen Ressourcengruppe, ihren Ressourcen und zugehörigen Richtlinien angezeigt:

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulersSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
ApplySnapvaultUpdate : False  
ApplyRetention : False  
RetentionCount : 0  
RetentionDays : 0  
ApplySnapMirrorUpdate : False  
SnapVaultLabel :  
MirrorVaultUpdateRetryCount : 7  
AppPolicies : {}  
Description : FinancePolicy  
PreScriptPath :  
PreScriptArguments :  
PostScriptPath :  
PostScriptArguments :  
ScriptTimeout : 60000  
DateModified : 8/4/2015 3:43:30 PM  
DateCreated : 8/4/2015 3:43:30 PM  
Schedule : SMCoreContracts.SmSchedule  
PolicyType : Backup  
PluginPolicyType : SMSQL  
Name : FinancePolicy  
Type :  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
clab-a13-13.sddev.lab.netapp.com  
DatabaseGUID :  
SQLInstance : clab-a13-13  
DbStatus : AutoClosed  
DbAccess : eUndefined  
IsSystemDb : False  
IsSimpleRecoveryMode : False  
IsSelectable : True  
SqlDbFileGroups : {}  
SqlDbLogFiles : {}

```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. Starten Sie einen Klonvorgang aus einer vorhandenen Sicherung mithilfe des Cmdlets New-SmClone.

Dieses Beispiel erstellt einen Klon aus einem angegebenen Backup mit allen Protokollen:

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

In diesem Beispiel wird ein Klon einer angegebenen Microsoft SQL Server-Instanz erstellt:

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. Zeigen Sie den Status des Klonauftrags mithilfe des Cmdlets Get-SmCloneReport an.

Dieses Beispiel zeigt einen Klonbericht für die angegebene Job-ID an:

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

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"](#) .

## Überwachen von IBM Db2-Klonvorgängen

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**.

## 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 <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme         | Wählen Sie <b>Pfad</b> 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 Klon 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"](#)

## Löschen oder Aufteilen von IBM Db2-Datenbankklonen nach dem Upgrade von SnapCenter

Nach dem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource aufteilen, aus der die Klone erstellt wurden.

#### Informationen zu diesem Vorgang

Wenn Sie den Speicherbedarf der versteckten Klone ermitteln möchten, führen Sie den folgenden Befehl aus:  
`Get-SmClone -ListStorageFootprint`

#### Schritte

1. Löschen Sie die Sicherungen der geklonten Ressourcen mithilfe des Cmdlets „remove-smbbackup“.
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mithilfe des Cmdlets „remove-smresourcegroup“.
3. Entfernen Sie den Schutz der geklonten Ressource mithilfe des Cmdlets „remove-smprotectresource“.
4. Wählen Sie die übergeordnete Ressource auf der Seite „Ressourcen“ aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht „Kopien verwalten“ die Klone entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.

6. Wählen Sie die Klone aus und klicken Sie dann auf  , um Klone zu löschen, oder klicken Sie auf  um die Klone zu teilen.
7. Klicken Sie auf **OK**.

# Schützen Sie PostgreSQL

## SnapCenter Plug-in für PostgreSQL

### Übersicht über das SnapCenter -Plug-in für PostgreSQL

Das SnapCenter -Plug-in für PostgreSQL-Cluster ist eine hostseitige Komponente der NetApp SnapCenter software , die eine anwendungsbewusste Datensicherungsverwaltung von PostgreSQL-Clustern ermöglicht. Das Plug-in für PostgreSQL-Cluster automatisiert die Sicherung, Wiederherstellung und das Klonen von PostgreSQL-Clustern in Ihrer SnapCenter Umgebung.

SnapCenter unterstützt PostgreSQL-Setups mit einem oder mehreren Clustern. Sie können das Plug-in für PostgreSQL-Cluster sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird PostgreSQL als manuelle Ressource unterstützt.

Wenn das Plug-in für PostgreSQL-Cluster installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen. Sie können das Plug-in auch mit der NetApp SnapVault -Technologie verwenden, um eine Disk-to-Disk-Backup-Replikation zur Einhaltung von Standards durchzuführen.

Das SnapCenter -Plug-in für PostgreSQL unterstützt NFS und SAN auf ONTAP und Azure NetApp Dateispeicherlayouts.

Das virtuelle Speicherlayout VMDK, vVol und RDM wird unterstützt.

### Was Sie mit dem SnapCenter Plug-in für PostgreSQL tun können

Wenn Sie das Plug-in für PostgreSQL-Cluster in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von PostgreSQL-Clustern und deren Ressourcen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Cluster hinzufügen.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

### SnapCenter Plug-in für PostgreSQL-Funktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit dem Plug-in für PostgreSQL-Cluster zu arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter .

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Kopiertechnologie**

SnapCenter verwendet die Snapshot-Technologie von NetApp mit dem Plug-in für PostgreSQL-Cluster, um Ressourcen zu sichern.

Die Verwendung des Plug-ins für PostgreSQL bietet außerdem die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung für die Consistency Group (CG)-Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Unterstützung für Linux LVM auf dem XFS-Dateisystem.

## **Vom SnapCenter Plug-in für PostgreSQL unterstützte Speichertypen**

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen Maschinen als auch auf virtuellen Maschinen (VMs). Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter -Plug-in für PostgreSQL installieren.

| Maschine          | Speichertyp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | <ul style="list-style-type: none"> <li>• FC-verbundene LUNs</li> <li>• Über iSCSI verbundene LUNs</li> <li>• Über NFS verbundene Volumes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| VMware ESXi       | <ul style="list-style-type: none"> <li>• RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt.</li> </ul> <p>Sie können die Datei <b>LinuxConfig.pm</b> unter <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> bearbeiten, um den Wert des Parameters <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> auf 1 zu setzen und nur die HBAs erneut zu scannen, die in HBA_DRIVER_NAMES aufgeführt sind.</p> <ul style="list-style-type: none"> <li>• iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind</li> <li>• VMDKs auf NFS-Datenspeichern</li> <li>• VMDKs auf VMFS</li> <li>• NFS-Volumes, die direkt mit dem Gastsystem verbunden sind</li> <li>• vVol-Datenspeicher auf NFS und SAN</li> </ul> <p>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p> |

## Für das PostgreSQL-Plug-In sind mindestens ONTAP Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN erstellen
  - LUN erstellen
  - LUN löschen

- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- LUN-Igroup umbenennen
- lun igroup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN persistent-reservation clear
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen

- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle anzeigen

## Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für PostgreSQL

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#) .

## Backup-Strategie für PostgreSQL

### Definieren Sie eine Sicherungsstrategie für PostgreSQL

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge verfügen Sie über die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

### Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

### Schritte



1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.
4. Entscheiden Sie, ob Sie eine auf Snapshot-Kopien basierende Richtlinie erstellen möchten, um anwendungskonsistente Snapshots des Clusters zu sichern.
5. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
6. Bestimmen Sie die Aufbewahrungsdauer für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
7. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

### **Automatische Erkennung von Ressourcen auf Linux-Hosts**

Ressourcen sind PostgreSQL-Cluster und -Instanzen auf dem Linux-Host, die von SnapCenter verwaltet werden. Nach der Installation des SnapCenter -Plug-ins für PostgreSQL werden die PostgreSQL-Cluster aller Instanzen auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.

### **Unterstützte Sicherungstypen**

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot-Kopien basierenden Sicherungstyp für PostgreSQL-Cluster.

#### **Snapshot-Kopie-basierte Sicherung**

Auf Snapshot-Kopien basierende Backups nutzen die Snapshot-Technologie von NetApp , um schreibgeschützte Online-Kopien der Volumes zu erstellen, auf denen sich die PostgreSQL-Cluster befinden.

### **So verwendet das SnapCenter Plug-in für PostgreSQL Konsistenzgruppen-Snapshots**

Sie können das Plug-In verwenden, um Konsistenzgruppen-Snapshots für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes aufnehmen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe besteht aus gleichzeitigen Snapshots mehrerer Volumes und bietet konsistente Kopien einer Volumengruppe.

Sie können auch die Wartezeit angeben, die der Speichercontroller benötigt, um Snapshots konsistent zu gruppieren. Die verfügbaren Wartezeitoptionen sind **Dringend**, **Mittel** und **Entspannt**. Sie können die WAFL-Synchronisierung (Write Anywhere File Layout) auch während des konsistenten Gruppen-Snapshot-Vorgangs aktivieren oder deaktivieren. Die WAFL Synchronisierung verbessert die Leistung eines Konsistenzgruppen-Snapshots.

### **So verwaltet SnapCenter die Datensicherung**

SnapCenter verwaltet die Datensicherungen auf Speichersystem- und Dateisystemebene.

Die Snapshots auf dem primären oder sekundären Speicher und die entsprechenden Einträge im PostgreSQL-

Katalog werden basierend auf den Aufbewahrungseinstellungen gelöscht.

## Überlegungen zur Festlegung von Sicherungszeitplänen für PostgreSQL

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen)

Die Sicherungshäufigkeit, bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen)

Sicherungszeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird.

## Anzahl der für PostgreSQL benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

## Sicherungsnamenskonventionen für Plug-in für PostgreSQL-Cluster

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.

- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: *customtext\_resourcegroup\_policy\_hostname* oder *resourcegroup\_hostname*. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

## Wiederherstellungs- und Recovery-Strategie für PostgreSQL

### Definieren Sie eine Wiederherstellungsstrategie für PostgreSQL-Ressourcen

Sie müssen vor der Wiederherstellung Ihres Clusters eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.



Es wird nur die manuelle Wiederherstellung des Clusters unterstützt.

#### Schritte

1. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für manuell hinzugefügte PostgreSQL-Ressourcen
2. Bestimmen Sie die unterstützten Wiederherstellungsstrategien für automatisch erkannte PostgreSQL-Cluster
3. Entscheiden Sie sich für die Art der Wiederherstellungsvorgänge, die Sie durchführen möchten.

### Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte PostgreSQL-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können.



Sie können manuell hinzugefügte PostgreSQL-Ressourcen nicht wiederherstellen.

### Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem für die Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

**HINWEIS:** Das Plug-in für PostgreSQL erstellt ein Backup-Label und eine Tablespace-Map im Ordner */<OS\_temp\_folder>/postgresql\_sc\_recovery<Restore\_JobId>/*, um die manuelle Wiederherstellung zu erleichtern.

### Art der unterstützten Wiederherstellungsstrategie für automatisch erkanntes PostgreSQL

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können.

Die vollständige Wiederherstellung von Ressourcen ist die unterstützte Wiederherstellungsstrategie für

automatisch erkannte PostgreSQL-Cluster. Dadurch werden alle Volumes, Qtrees und LUNs einer Ressource wiederhergestellt.

### Arten von Wiederherstellungsvorgängen für automatisch erkanntes PostgreSQL

Das SnapCenter -Plug-in für PostgreSQL unterstützt Single File SnapRestore und Connect-and-Copy-Wiederherstellungstypen für automatisch erkannte PostgreSQL-Cluster.

**Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:**

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das ausgewählte Backup von einem SnapMirror oder SnapVault Sekundärspeicherort stammt und die Option **Complete Resource** ausgewählt ist

**Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien durchgeführt:**

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das Backup von einem SnapMirror oder SnapVault Sekundärspeicherort ausgewählt wird und die Option **Complete Resource** ausgewählt ist

### Für PostgreSQL-Cluster unterstützte Arten von Wiederherstellungsvorgängen

Mit SnapCenter können Sie verschiedene Arten von Wiederherstellungsvorgängen für PostgreSQL-Cluster durchführen.

- Wiederherstellen des Clusters bis zum aktuellsten Stand
- Wiederherstellen des Clusters bis zu einem bestimmten Zeitpunkt

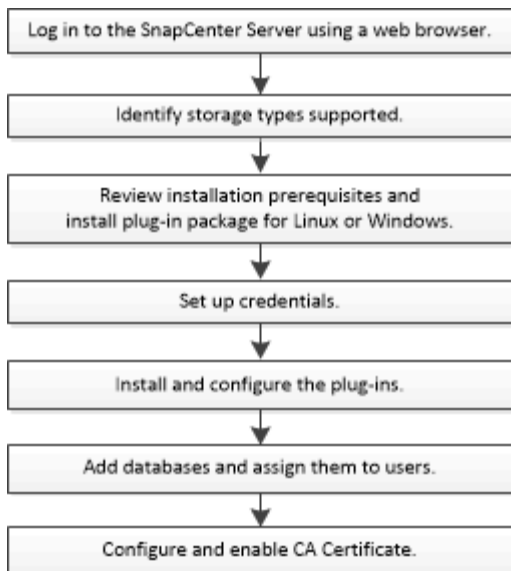
Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.

SnapCenter bietet auch die Option „Keine Wiederherstellung“ für PostgreSQL-Cluster.

## Vorbereiten der Installation des SnapCenter Plug-ins für PostgreSQL

### Installationsablauf des SnapCenter Plug-ins für PostgreSQL

Sie sollten das SnapCenter Plug-in für PostgreSQL installieren und einrichten, wenn Sie PostgreSQL-Cluster schützen möchten.



## Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für PostgreSQL

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Das SnapCenter Plug-in für PostgreSQL ist sowohl in Windows- als auch in Linux-Umgebungen verfügbar.

- Sie müssen Java 11 auf Ihrem Host installiert haben.



IBM Java wird auf Windows- und Linux-Hosts nicht unterstützt.

- Unter Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „LocalSystem“ ausgeführt werden. Dies ist das Standardverhalten, wenn das Plug-in für PostgreSQL als Domänenadministrator installiert wird.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren. Das SnapCenter -Plug-in für Microsoft Windows wird standardmäßig mit dem PostgreSQL-Plug-in auf Windows-Hosts bereitgestellt.
- Der SnapCenter -Server sollte Zugriff auf den 8145- oder benutzerdefinierten Port des Plug-ins für den PostgreSQL-Host haben.

### Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Während der Installation des Plug-ins für PostgreSQL auf einem Windows-Host wird das SnapCenter -Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Windows-Host installiert haben.

["Laden Sie JAVA für alle Betriebssysteme herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

## Linux-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

["Laden Sie JAVA für alle Betriebssysteme herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Bei PostgreSQL-Clustern, die auf einem Linux-Host ausgeführt werden, wird bei der Installation des Plug-ins für PostgreSQL automatisch das SnapCenter Plug-in für UNIX installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

## Ergänzende Befehle

Um einen zusätzlichen Befehl im SnapCenter -Plug-in für PostgreSQL auszuführen, müssen Sie ihn in die Datei *allowed\_commands.config* aufnehmen.

- Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*

Um zusätzliche Befehle auf dem Plug-In-Host zuzulassen, öffnen Sie die Datei *allowed\_commands.config* in einem Editor. Geben Sie jeden Befehl in einer separaten Zeile ein. Bei den Befehlen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen (") einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: mount Befehl: umount Befehl: "C:\Programme\ NetApp\SnapCreator commands\sdcli.exe" Befehl: myscript.bat

Wenn die Datei *allowed\_commands.config* nicht vorhanden ist, werden die Befehle oder die Skriptausführung blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."

Wenn der Befehl oder das Skript nicht in der Datei „*allowed\_commands.config*“ vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."



Um alle Befehle zuzulassen, sollten Sie keinen Platzhaltereintrag (\*) verwenden.

## Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host

SnapCenter ermöglicht einem Nicht-Root-Benutzer, das SnapCenter -Plug-In-Paket für Linux zu installieren und den Plug-In-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

## Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- `/home/LINUX_USER/sc_netapp/snapcenter_linux_host_plugin.bin`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/bin/spl`

## Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei `/etc/sudoers` hinzu.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

*LINUX\_USER* ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei **sc\_unix\_plugins\_checksum.txt** abrufen, die sich hier befindet:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` \_ wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` \_ wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel         | Anforderungen                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |



| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <div> <div>5 GB</div> <div>  <p>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.</p> </div> </div> |
| Erforderliche Softwarepakete                                                                 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                                            |

## Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux

Bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren, sollten Sie mit einigen grundlegenden Anforderungen an Speicherplatz und Größe des Hostsystems vertraut sein.

| Artikel                                              | Anforderungen                                                                                                                                                                                                                                                   |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                      | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host | 1 GB                                                                                                                                                                                                                                                            |

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>2 GB</p> <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | <p>Java 11 Oracle Java und OpenJDK</p> <p>Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                 |

## Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für PostgreSQL

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Clustern oder Windows-Dateisystemen erstellen.

### Informationen zu diesem Vorgang

- Linux-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldeinformationen für den Root-Benutzer oder für einen Nicht-Root-Benutzer mit Sudo-Berechtigungen einrichten, um den Plug-In-Prozess zu installieren und zu starten.

**Best Practice:** Obwohl Sie Anmeldeinformationen für Linux erstellen dürfen, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

- Windows-Hosts

Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.

Sie müssen die Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die zum Konfigurieren der Anmeldeinformationen erforderlichen Informationen an:

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |

| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername                      | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i></p> <p>Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (&lt;) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als &lt;!10, kleiner als 10 &lt;!, Backtick `12.</p> |
| Passwort                          | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Authentifizierungsmodus           | Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen <b>Sudo-Berechtigungen verwenden</b>, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p> <div data-bbox="873 1837 928 1894">  </div> <p>Gilt nur für Linux-Benutzer.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

## Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

### Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -Effectivelmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$  
.. Fügen Sie der Gruppe Computerobjekte hinzu.  
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des Dienstkontos.
```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:

- a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                |
|---------|----------------|-----------|-----------------------------------------------|
| -----   | -----          | -----     | -----                                         |
| True    | No             | Success   | {Active Directory Domain Services, Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- Starten Sie Ihren Host neu.
  - Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
  - Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
- Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
  - Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Installieren Sie das SnapCenter -Plug-in für PostgreSQL

### Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert. Sie können den Host hinzufügen und Plug-In-Pakete für einen einzelnen Host installieren.

#### Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zur Verwaltung von Hosts.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

["Konfigurieren Sie ein gruppenverwaltetes Dienstkonto auf Windows Server 2016 oder höher für PostgreSQL"](#)

### Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.

### 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            | <p>Wählen Sie den Hosttyp aus:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> </ul> <div>  <p>Das Plug-in für PostgreSQL wird auf dem PostgreSQL-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> </div> |
| Hostname           | <p>Geben Sie den Hostnamen für die Kommunikation ein. Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p>                                                                                                       |

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationen | <p>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.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div>  <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

Wenn Sie die REST-API zum Installieren des Plug-ins für PostgreSQL verwenden, müssen Sie die Version als 3.0 übergeben. Beispiel: PostgreSQL:3.0

6. (Optional) Klicken Sie auf **Weitere Optionen**.

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen              | <p>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.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |



| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installationspfad                                                                           | <p>Das Plug-in für PostgreSQL wird auf dem PostgreSQL-Clienthost installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> <ul style="list-style-type: none"> <li>Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter. Optional können Sie den Pfad anpassen.</li> <li>Für das SnapCenter Plug-ins-Paket für Linux ist der Standardpfad /opt/ NetApp/snapcenter. Optional können Sie den Pfad anpassen.</li> </ul>                                                                            |
| Vorinstallationsprüfungen überspringen                                                      | 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.                                                                                                                                                                                                                                                                                                                                                                    |
| Alle Hosts im Cluster hinzufügen                                                            | Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten hinzuzufügen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | <p>Aktivieren Sie für Windows-Hosts dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.</p> <div>  <p>Geben Sie den gMSA-Namen im folgenden Format an:<br/>Domänenname\Kontoname\$.</p> </div> <div>  <p>gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.</p> </div> |

## 7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-Ins) und Java-Version (für Linux-Plug-Ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, 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, müssen Sie das Problem beheben.



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

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



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

9. Überwachen Sie den Installationsfortschritt.

- Für Windows-Plug-Ins befinden sich die Installations- und Upgrade-Protokolle unter: `C:\Windows\SnapCenter plugin\Install<JOBID>\_`
- Für Linux-Plug-Ins befinden sich die Installationsprotokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_` und die Upgrade-Protokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

## Installieren Sie SnapCenter Plug-in-Pakete für Linux oder Windows auf mehreren Remote-Hosts mithilfe von Cmdlets

Sie können die SnapCenter -Plug-in-Pakete für Linux oder Windows mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

### Bevor Sie beginnen

Sie müssen sich auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-In auf mehreren Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

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"](#) .

Sie können die Option `-skippercheck` verwenden, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

## Installieren Sie das SnapCenter -Plug-in für PostgreSQL auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle

Sie sollten das SnapCenter Plug-in für PostgreSQL-Cluster mithilfe der SnapCenter Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des

Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie das Plug-In für PostgreSQL-Cluster entweder im Konsolenmodus oder im Hintergrundmodus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

### Bevor Sie beginnen

- Sie sollten das Plug-in für PostgreSQL-Cluster auf jedem Linux-Host installieren, auf dem sich der PostgreSQL-Client befindet.
- Der Linux-Host, auf dem Sie das SnapCenter -Plug-in für den PostgreSQL-Cluster installieren, muss die abhängigen Software-, Cluster- und Betriebssystemanforderungen erfüllen.

Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den unterstützten Konfigurationen.

#### ["NetApp Interoperabilitätsmatrix-Tool"](#)

- Das SnapCenter -Plug-in für PostgreSQL-Cluster ist Teil des SnapCenter Plug-in-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins-Paket für Linux installieren, sollten Sie SnapCenter bereits auf einem Windows-Host installiert haben.

### Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter Plug-ins-Pakets für Linux (snapcenter\_linux\_host\_plugin.bin) von C:\ProgramData\NetApp\ SnapCenter\Package Repository auf den Host, auf dem Sie das Plug-in für PostgreSQL installieren möchten.

Sie können auf diesen Pfad von dem Host aus zugreifen, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei kopiert haben.

3. Installieren Sie das Plug-In:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT gibt den SMCore HTTPS-Kommunikationsport an.
- -DSERVER\_IP gibt die IP-Adresse des SnapCenter -Servers an.
- -DSERVER\_HTTPS\_PORT gibt den HTTPS-Port des SnapCenter -Servers an.
- -DUSER\_INSTALL\_DIR gibt das Verzeichnis an, in dem Sie das SnapCenter Plug-Ins-Paket für Linux installieren möchten.
- DINSTALL\_LOG\_NAME gibt den Namen der Protokolldatei an.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Bearbeiten Sie die Datei /<Installationsverzeichnis>/NetApp/snapcenter/scc/etc/SC\_SMS\_Services.properties und fügen Sie dann den Parameter PLUGINS\_ENABLED = PostgreSQL:3.0 hinzu.

5. Fügen Sie den Host mit dem Cmdlet Add-Smhost und den erforderlichen Parametern zum SnapCenter -Server hinzu.

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 ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Überwachen Sie den Status der Installation des Plug-ins für PostgreSQL

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#) .



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

## CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

### Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

#### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
  - a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-ChildItem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

### Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

#### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## Konfigurieren Sie das CA-Zertifikat für den SnapCenter PostgreSQL Plug-Ins-Dienst auf dem Linux-Host

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

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter `/opt/NetApp/snapcenter/scc/etc` befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Dies ist der Wert, der dem Schlüssel „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_in_cert" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE\_PASS in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

#### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder  
Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

#### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```



5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.

7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE\_PASS in der Datei agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei agent.properties.

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC\_CERTIFICATE\_ALIAS.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

#### Informationen zu diesem Vorgang

- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-Ins ist „opt/NetApp/snapcenter/scc/etc/crl“.

#### Schritte

1. Sie können das Standardverzeichnis in der Datei agent.properties anhand des Schlüssels CRL\_PATH ändern und aktualisieren.

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

### Konfigurieren Sie das CA-Zertifikat für den SnapCenter PostgreSQL Plug-Ins-Dienst auf dem Windows-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-

In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter -Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-ins verwenden die Datei *keystore.jks*, die sich unter *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc* befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Es handelt sich um den Wert, der dem Schlüssel *KEYSTORE\_PASS* entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

```
C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

```
keytool -keypasswd -alias "Aliasname_im_Zertifikat" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel *KEYSTORE\_PASS* in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „*keystore.jks*“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

#### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher `C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc`
2. Suchen Sie die Datei `keystore.jks`.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels `KEYSTORE_PASS` in der Datei `agent.properties`.

```
keytool -keypasswd -alias "Aliasname_im_CA_Zertifikat" -keystore keystore.jks
```

8. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei `agent.properties`.

Aktualisieren Sie diesen Wert anhand des Schlüssels `SCC_CERTIFICATE_ALIAS`.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter -Plug-Ins

#### Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe ["So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat"](#) .
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.

- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist 'C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\crl'.

### Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* anhand des Schlüssels 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.

## Bereiten Sie sich auf den Datenschutz vor

## Voraussetzungen für die Verwendung des SnapCenter -Plug-Ins für PostgreSQL

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

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich beim SnapCenter -Server an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen und gegebenenfalls Anmeldeinformationen erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

Sie müssen den Java-Pfad in der Umgebungspfadvariable des Hostcomputers festlegen.

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.

## Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von PostgreSQL verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei den Ressourcen handelt es sich normalerweise um PostgreSQL-Cluster, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Sicherungshäufigkeit, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

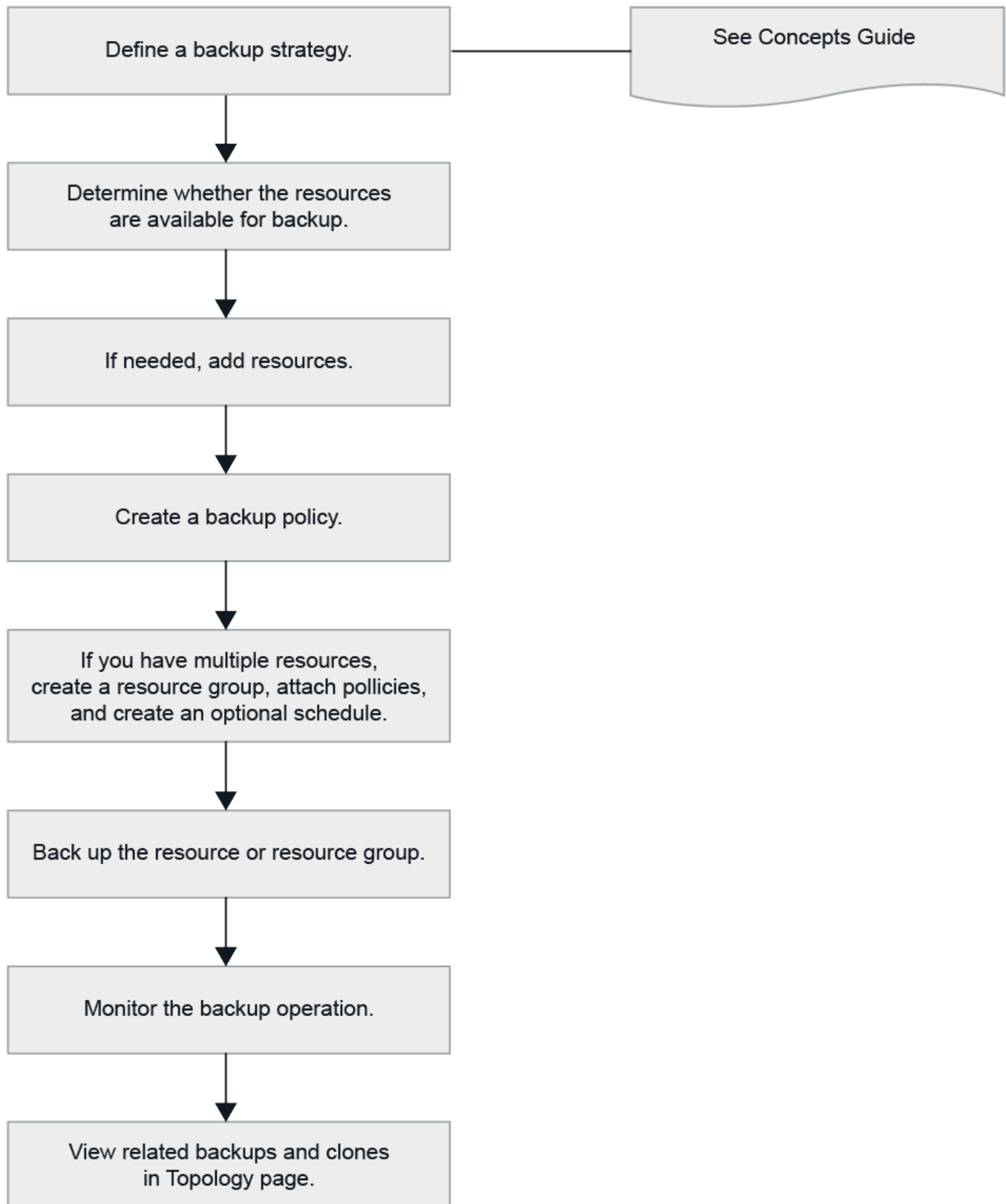
Stellen Sie sich eine Ressourcengruppe so vor, dass sie definiert, was Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als ob sie definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Cluster sichern, können Sie eine Ressourcengruppe erstellen, die alle Cluster im Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird.

# Sichern von PostgreSQL-Ressourcen

## Sichern von PostgreSQL-Ressourcen

Sie können entweder eine Sicherung einer Ressource (Cluster) oder einer Ressourcengruppe erstellen. Der Sicherungsworkflow umfasst die Planung, die Identifizierung der Cluster für die Sicherung, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets. ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

## Automatisches Erkennen der Cluster

Ressourcen sind PostgreSQL-Cluster auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren PostgreSQL-Cluster ermittelt haben.

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen abgeschlossen haben.
- Das SnapCenter -Plug-in für PostgreSQL unterstützt keine automatische Erkennung der Ressourcen, die sich in virtuellen RDM/VMDK-Umgebungen befinden.

### Informationen zu diesem Vorgang

- Nach der Installation des Plug-ins werden alle Cluster auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.
- Nur Cluster werden automatisch erkannt.

Die automatisch erkannten Ressourcen können nicht geändert oder gelöscht werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für PostgreSQL aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste „Anzeigen“ aus.
3. (Optional) Klicken Sie auf  \* und wählen Sie dann den Hostnamen aus.

Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen anzuzeigen.

Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

- Wenn sich der Cluster auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt.
- Wenn sich der Cluster auf einem NetApp -Speichersystem befindet und geschützt ist und kein Sicherungsvorgang ausgeführt wird, wird in der Spalte „Gesamtstatus“ die Meldung „Sicherung nicht ausgeführt“ angezeigt. Andernfalls ändert sich der Status basierend auf dem letzten Sicherungsstatus in „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“.



Sie müssen die Ressourcen aktualisieren, wenn die Cluster außerhalb von SnapCenter umbenannt werden.

## Ressourcen manuell zum Plug-In-Host hinzufügen

Die automatische Erkennung wird auf Windows-Hosts nicht unterstützt. Sie müssen Postgresql-Clusterressourcen manuell hinzufügen.

### Bevor Sie beginnen



- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten von Speichersystemverbindungen abgeschlossen haben.

### Informationen zu diesem Vorgang

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

### Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter Plug-in für Postgresql aus der Dropdown-Liste aus und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite „Ressourcen“ auf **Postgresql-Ressourcen hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Name                 | Geben Sie den Clusternamen an.                                                                                                    |
| Hostname             | Geben Sie den Hostnamen ein.                                                                                                      |
| Typ                  | Cluster auswählen.                                                                                                                |
| Beispiel             | Geben Sie den Namen der Instanz an, die dem Cluster übergeordnet ist.                                                             |
| Anmeldeinformationen | Wählen Sie die Anmeldeinformationen aus oder fügen Sie Informationen zu den Anmeldeinformationen hinzu.<br><br>Dies ist optional. |

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ einen Speichertyp und ein oder mehrere Volumes, LUNs und Qtrees aus und klicken Sie dann auf **Speichern**.

Optional: Sie können auf das \* klicken  \* Symbol zum Hinzufügen weiterer Volumes, LUNs und Qtrees aus anderen Speichersystemen.

5. Optional: Geben Sie auf der Seite „Ressourceneinstellungen“ für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für das PostgreSQL-Plug-In ein.
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Die Cluster werden zusammen mit Informationen wie dem Hostnamen, den zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie die Ressourcen den Benutzern zuweisen. Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

["Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"](#)

## Nach Abschluss

- Nachdem Sie die Cluster hinzugefügt haben, können Sie die PostgreSQL-Clusterdetails ändern.
- Die migrierten Ressourcen (Tablespace und Cluster) von SnapCenter 5.0 werden in SnapCenter 6.0 als PostgreSQL-Clustertyp gekennzeichnet.
- Wenn Sie die manuell hinzugefügten Ressourcen ändern, die von SnapCenter 5.0 oder früher migriert wurden, gehen Sie auf der Seite **Ressourceneinstellungen** für benutzerdefinierte Schlüssel-Wert-Paare wie folgt vor:
  - Geben Sie im Feld **Name** den Begriff „PORT“ ein.
  - Geben Sie die Portnummer im Feld **Wert** an.

## Erstellen von Sicherungsrichtlinien für PostgreSQL

Bevor Sie SnapCenter zum Sichern von PostgreSQL-Ressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren.

### Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für PostgreSQL-Cluster.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen von Ressourcen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

Darüber hinaus können Sie in der Richtlinie Replikations-, Skript- und Anwendungseinstellungen angeben. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

### 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. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie den Speichertyp aus.
  - b. Geben Sie im Abschnitt **Benutzerdefinierte Sicherungseinstellungen** alle spezifischen Sicherungseinstellungen an, die im Schlüssel-Wert-Format an das Plug-In übergeben werden müssen.  
  
Sie können mehrere Schlüsselwerte angeben, die an das Plug-In übergeben werden sollen.
6. Führen Sie auf der Seite „Sicherung und Replikation“ die folgenden Aktionen aus:
  - a. Geben Sie die Zeitplanhäufigkeit an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber auch jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- a. Geben Sie im Abschnitt „Snapshot-Einstellungen“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

| Wenn Sie wollen...                                                 | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Snapshots                   | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> <div>  <p>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.</p> </div> <div>  <p>Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der ONTAP -Version unterstützt wird.</p> </div> |
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Sperrzeitraum für Snapshot-Kopien                                  | <p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopien</b> und geben Sie Tage, Monate oder Jahre an.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

#### 7. Wählen Sie eine 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.

#### 8. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden

sekundären Replikationsoptionen aus:

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b> | <p>Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation).</p> <p>Wenn die Schutzbeziehung in ONTAP vom Typ „Mirror und Vault“ ist und Sie nur diese Option auswählen, wird der auf dem primären Server erstellte Snapshot nicht zum Ziel übertragen, sondern im Ziel aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird die folgende Fehlermeldung angezeigt: „Der sekundäre Speicherort ist für die ausgewählte gewölbte/gespiegelte Sicherung nicht verfügbar.“</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen von Backups und Klonen im Zusammenhang mit PostgreSQL-Ressourcen auf der Seite „Topologie“"</a> .</p> |

| Für dieses Feld...                                                                         | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b> | <p>Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.</p> <p>Weitere Informationen zu SnapLock Vault finden Sie unter Commit Snapshots to WORM on a vault destination</p> <p>Sehen <a href="#">"Anzeigen von Backups und Klonen im Zusammenhang mit PostgreSQL-Ressourcen auf der Seite „Topologie“"</a> .</p> |
| <b>Fehler bei der Wiederholungsanzahl</b>                                                  | Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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

## Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### Informationen zu diesem Vorgang

- 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 **Ressourcen** und wählen Sie dann 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:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | <p>Geben Sie einen Namen für die Ressourcengruppe ein.</p> <div><p>Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</p></div>                                                                                                     |
| Schlagwörter                                                  | <p>Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.</p> <p>Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.</p>                                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | <p>Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.</p> <p>Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p> |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

Dies hilft, Informationen auf dem Bildschirm zu filtern.

5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:
  - a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                             | Machen Sie Folgendes...                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Snapshot-Vorgangs der Konsistenzgruppe zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs anzugeben.<br><br>Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                            | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

+

- Klicken Sie auf den Pfeil **Skripts** 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.
- Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

| Parameter         | Einstellung | Beschreibung                                                              |
|-------------------|-------------|---------------------------------------------------------------------------|
| ARCHIV_LOG_ENABLE | (J/N)       | Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle. |



| Parameter                     | Einstellung                | Beschreibung                                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIV_LOG_RETENTION          | Anzahl_der_Tage            | Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden.<br><br>Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein.                                                                                              |
| ARCHIVE_LOG_DIR               | change_info_directory/logs | Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.                                                                                                                                                                                           |
| ARCHIVE_LOG_EXT               | Dateierweiterung           | Gibt die Erweiterungslänge der Archivprotokolldatei an.<br><br>Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.161518551942 9 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (J/N)                      | Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen.<br><br>Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.                                                                        |



Die benutzerdefinierten Schlüssel-Wert-Paare werden für PostgreSQL-Linux-Plug-in-Systeme unterstützt und nicht für PostgreSQL-Cluster, die als zentralisiertes Windows-Plug-in registriert sind.

- c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                                                                        | Dann...                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar. | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*. |

| Falls Sie es wollen...                                                                              | Dann...                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                          | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                                                                     |
| Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot-Kopien zu erstellen. | Wählen Sie <b>Andere</b> aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen. |

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

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



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

Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

- b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \* \* für die Richtlinie, die Sie konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist „policy\_name“ 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. Der SMTP-Server muss unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für PostgreSQL-Ressourcen 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                  |
|------------------------------------------------------|----------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> . |

| Wenn Sie wollen...          | Machen Sie Folgendes...                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Planen Sie eine Überprüfung | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Erstellen Sie eine Speichersystemverbindung und eine Anmeldeinformation mit PowerShell-Cmdlets für PostgreSQL

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern, Wiederherstellen oder Klonen von PostgreSQL-Clustern verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Clusterstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

### Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

Dieses Beispiel zeigt, wie Sie mit Windows-Anmeldeinformationen neue Anmeldeinformationen mit dem Namen „FinanceAdmin“ erstellen:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. Fügen Sie den PostgreSQL-Kommunikationshost zum SnapCenter -Server hinzu.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode PostgreSQL
```

5. Installieren Sie das Paket und das SnapCenter -Plug-in für PostgreSQL auf dem Host.

Für Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
PostgreSQL
```

Für Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
PostgreSQL -FileSystemCode scw -RunAsName FinanceAdmin
```

6. Legen Sie den Pfad zur SQLLIB fest.

Für Windows verwendet das PostgreSQL-Plug-In den Standardpfad für den SQLLIB-Ordner:  
„C:\Programme\IBM\SQLLIB\BIN“.

Wenn Sie den Standardpfad überschreiben möchten, verwenden Sie den folgenden Befehl.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode PostgreSQL -configSettings @{ "PostgreSQL_SQLLIB_CMD" = "<custom_path>\IBM\SQLLIB\BIN" }
```

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"](#) .

## Sichern Sie PostgreSQL

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Stellen Sie bei Sicherungsvorgängen auf Basis von Snapshot-Kopien sicher, dass alle Mandantencluster gültig und aktiv sind.
- Bei Pre- und Post-Befehlen für Quiesce-, Snapshot- und Unquiesce-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Wählen \*\* und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- Wählen Sie den Pfeil **Backups** aus, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                            | Machen Sie Folgendes...                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Vorgangs „Consistency Group Snapshot“ zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für die Fertigstellung des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                           | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

- Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.

Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

- Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:



| Falls Sie es wollen...                                                                                                                                   | Dann...                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                               | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                      |
| SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.                                       |
| So geben Sie den Befehl zum Erstellen eines Snapshots ein                                                                                                | Wählen Sie <b>Andere</b> und geben Sie dann den Befehl zum Erstellen eines Snapshots ein. |

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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

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

- b. Wählen \* \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

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

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Wählen Sie **Jetzt sichern**.

10. 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. Wählen Sie **Backup**.

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

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl.

Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript startet der Befehl `do_start method` den SnapCenter VMware-Plug-in-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-SmConnection
```

Die Eingabeaufforderung für Benutzernamen und Kennwort wird angezeigt.

2. Fügen Sie mithilfe des Cmdlets `Add-SmResources` manuelle Ressourcen hinzu.

Dieses Beispiel zeigt, wie eine PostgreSQL-Instanz hinzugefügt wird:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.
4. Schützen Sie die Ressource oder fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.
5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert wird:

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
-Policy postgresql_policy1
```

In diesem Beispiel wird eine geschützte Ressource gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
-Policy postgresql_policy2
```

6. Überwachen Sie den Auftragsstatus (wird ausgeführt, abgeschlossen oder fehlgeschlagen) mithilfe des Cmdlets Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Überwachen Sie die Details des Sicherungsauftrags wie Sicherungs-ID und Sicherungsname, um mithilfe des Cmdlets Get-SmBackupReport Wiederherstellungs- oder Klonvorgänge durchzuführen.

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :

```

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"](#) .

## Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

### Informationen zu diesem Vorgang

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie  und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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. Wählen Sie **Backup**.

5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Überwachen von PostgreSQL-Sicherungsvorgängen

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 Sie Datenschutzvorgänge auf PostgreSQL-Clustern 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.

## Abbrechen von Sicherungsvorgängen für PostgreSQL

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.

- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

## Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"> <li>a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li> <li>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b>.</li> </ol>                                                                                                                                                                         |
| Aktivitätsbereich | <ol style="list-style-type: none"> <li>a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li> <li>b. Wählen Sie den Vorgang aus.</li> <li>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li> </ol> |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## Anzeigen von PostgreSQL-Sicherungen und -Klonen auf der Seite „Topologie“

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

### Informationen zu diesem Vorgang

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.

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

### 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 **Zusammenfassungskarte**, um eine Zusammenfassung der Anzahl der auf dem primären und sekundären Speicher verfügbaren Backups und Klone anzuzeigen.

Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Klone an.

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 die Anwendungsressource auf 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.

Nach der On-Demand-Sicherung werden durch Klicken auf die Schaltfläche **Aktualisieren** die Details der Sicherung oder des Klons aktualisiert.

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.

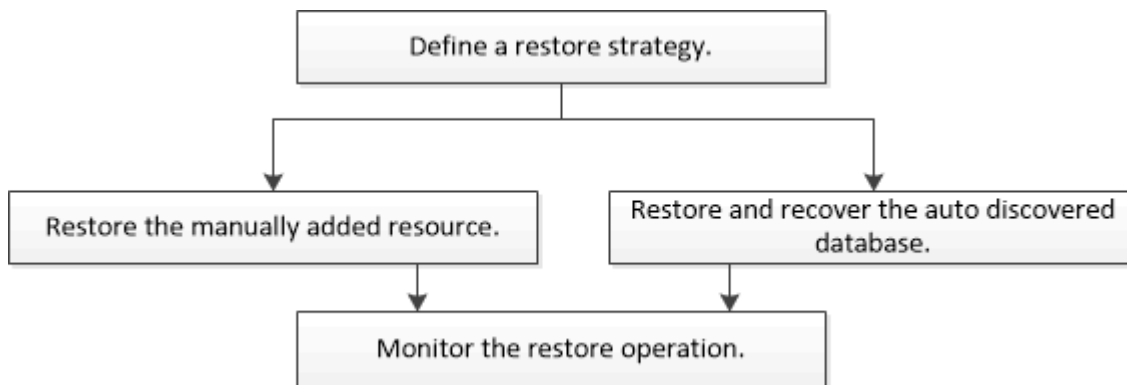
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

## PostgreSQL wiederherstellen

### Wiederherstellungs-Workflow

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

### Wiederherstellen und Wiederherstellen einer manuell hinzugefügten Ressourcensicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

#### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:

- Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

#### **Informationen zu diesem Vorgang**

- 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.



| Primary Backup(s)                           |                     |
|---------------------------------------------|---------------------|
| Backup Name                                 | End Date            |
| rg1_scpr0191685001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option **Vollständige Ressource** aus.
  - a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumes des PostgreSQL-Clusters wiederhergestellt.

Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

Sie können mehrere LUNs auswählen.



Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, Qtrees oder LUNs wiederhergestellt.

7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Befehle zum Aufheben der Bereitstellung verfügbar.

8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle verfügbar.

9. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

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

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime | BackupType |
|----------|-------------------------------|------------|------------|
| -----    | -----                         | -----      | -----      |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:02:32   |
| AM       | Full Backup                   |            |            |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:23:17   |
| AM       |                               |            |            |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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"](#) .

## Wiederherstellen und Wiederherstellen einer automatisch erkannten Clustersicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung

sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:

- Standardspeicherort auf dem Windows-Host: `C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Standardspeicherort auf dem Linux-Host: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Dateibasierte Sicherungskopien können nicht aus SnapCenter wiederhergestellt werden.
- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Die automatische Wiederherstellung wird nicht unterstützt.
- 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 **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                            |                                                                                                         |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------|
| search                                       |                        |
| Backup Name                                  | End Date                                                                                                |
| rg1_scspr0191683001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

- Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option „Vollständige Ressource“ aus, um die konfigurierten Datenvolumen des PostgreSQL-Clusters wiederherzustellen.
- Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:

| Wenn du...                                                       | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Möchten Sie so nah wie möglich an die aktuelle Zeit zurückkehren | Wählen Sie <b>Auf den letzten Zustand wiederherstellen</b> . Geben Sie für einzelne Containerressourcen einen oder mehrere Protokoll- und Katalogsicherungspeicherorte an.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Möchten Sie den angegebenen Zeitpunkt wiederherstellen           | Wählen Sie <b>Zu einem bestimmten Zeitpunkt wiederherstellen</b> .<br><br>a. Geben Sie Datum und Uhrzeit ein. Geben Sie Datum und Uhrzeit ein. Beispielsweise befindet sich der PostgreSQL-Linux-Host in Sunnyvale, Kalifornien, und der Benutzer in Raleigh, North Carolina, stellt die Protokolle in SnapCenter wieder her.<br><br>Wenn der Benutzer eine Wiederherstellung auf 5 Uhr morgens in Sunnyvale, CA durchführen möchte, muss er die Zeitzone des Browsers auf die Zeitzone des PostgreSQL Linux-Hosts (GMT-07:00) einstellen und Datum und Uhrzeit als 5:00 Uhr morgens angeben. |
| Will nicht erholen                                               | Wählen Sie <b>Keine Wiederherstellung</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



Sie können manuell hinzugefügte PostgreSQL-Ressourcen nicht wiederherstellen.



Das SnapCenter -Plug-in für PostgreSQL erstellt ein Backup-Label und eine Tablespace-Map im Ordner `<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/_`, um die manuelle Wiederherstellung zu erleichtern.

- Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Befehle zum Aufheben der Bereitstellung verfügbar.

- Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.



Für automatisch erkannte Ressourcen sind keine Mount-Befehle verfügbar.

3. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

4. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets

Das Wiederherstellen einer Ressourcensicherung umfasst das Einleiten einer Verbindungssitzung mit dem SnapCenter -Server, das Auflisten der Sicherungen und Abrufen von Sicherungsinformationen sowie das Wiederherstellen einer Sicherung.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „`Get-SmBackup`“ und „`Get-SmBackupReport`“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId    | BackupName                    | BackupTime           |
|-------------|-------------------------------|----------------------|
| BackupType  |                               |                      |
| -----       | -----                         | -----                |
| -----       |                               |                      |
| 1           | Payroll Dataset_vise-f6_08... | 8/4/2015 11:02:32 AM |
| Full Backup |                               |                      |
| 2           | Payroll Dataset_vise-f6_08... | 8/4/2015 11:23:17 AM |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDateTime "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :

```

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"](#).

## Überwachen von PostgreSQL-Wiederherstellungsvorgängen

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 von PostgreSQL-Ressourcensicherungen

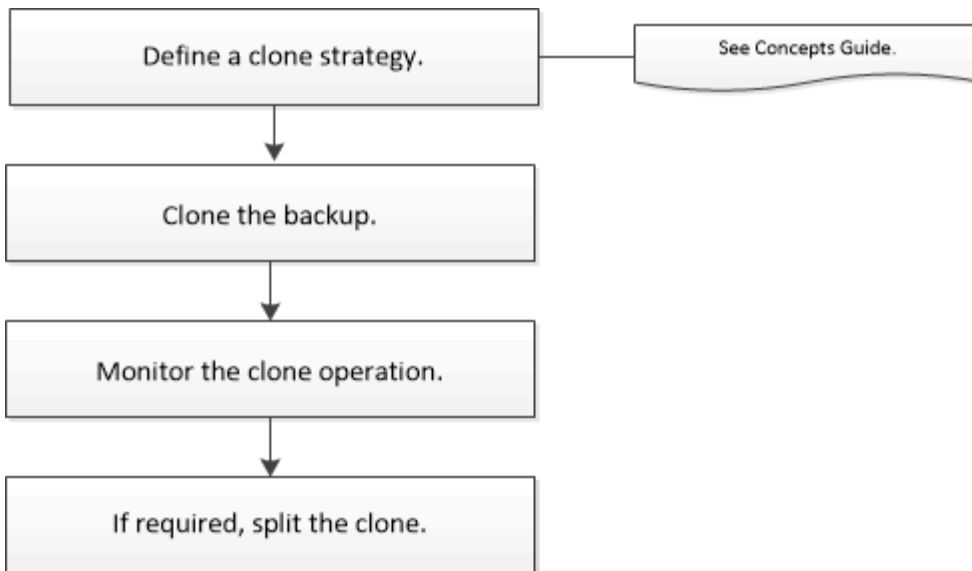
### Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

#### Informationen zu diesem Vorgang

- Sie können auf dem Quell-PostgreSQL-Server klonen.
- Sie können Ressourcensicherungen aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Für Datenextraktions- und Manipulationstools beim Befüllen von Data Warehouses
  - So stellen Sie versehentlich gelöschte oder geänderte Daten wieder her

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

## Klonen einer PostgreSQL-Sicherung

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen.

### Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Bei Befehlen vor oder nach dem Klonen sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: `C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
  - Standardspeicherort auf dem Linux-Host: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume"] .
- 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:

| Für dieses Feld...                         | Machen Sie Folgendes...                                                                                                                                  |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server klonen                              | Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.                                                                                        |
| Zielport                                   | Geben Sie den PostgreSQL-Zielport ein, um aus den vorhandenen Sicherungen zu klonen.                                                                     |
| NFS-Export-IP-Adresse                      | Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden.<br><br>Dies gilt nur für Ressourcen des NFS-Speichertyps. |
| Max. Durchsatz des Kapazitätspools (MiB/s) | Geben Sie den maximalen Durchsatz eines Kapazitätspools ein.<br><br>Dies gilt nur für Ressourcen des Speichertyps ANF.                                   |

7. Führen Sie auf der Seite „Skripts“ die folgenden Schritte aus:



Die Skripte werden auf dem Plug-in-Host ausgeführt.

- a. Geben Sie die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
  - Befehl vor dem Klonen: Löschen Sie vorhandene Cluster mit demselben Namen

- Befehl nach dem Klonen: Überprüfen Sie einen Cluster oder starten Sie einen Cluster.
- b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Mount-Befehl für ein Volume oder einen Qtree auf einer Linux-Maschine:

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer.

```
PS C:\> Open-SmConnection
```

2. Rufen Sie die Sicherungen ab, um den Klonvorgang mithilfe des Cmdlets „`Get-SmBackup`“ durchzuführen.

Dieses Beispiel zeigt, dass zwei Sicherungen zum Klonen verfügbar sind:

```
C:\PS> Get-SmBackup
```

| BackupId             | BackupName                    |
|----------------------|-------------------------------|
| BackupTime           | BackupType                    |
| -----                | -----                         |
| 1                    | Payroll Dataset_vise-f6_08... |
| 8/4/2015 11:02:32 AM | Full Backup                   |
| 2                    | Payroll Dataset_vise-f6_08... |
| 8/4/2015 11:23:17 AM |                               |

3. Starten Sie einen Klonvorgang von einer vorhandenen Sicherung und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

Dieses Beispiel zeigt, dass das zu klonende Backup eine `NFSExportIPs`-Adresse von 10.32.212.14 hat:

Für PostgreSQL-Cluster:

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```



Wenn NFSExportIPs nicht angegeben ist, wird der Standardwert auf den Klonzielhost exportiert.

- Überprüfen Sie, ob die Sicherungen erfolgreich geklont wurden, indem Sie mit dem Cmdlet „Get-SmCloneReport“ die Details des Klonauftrags anzeigen.

Sie können Details wie Klon-ID, Startdatum und -uhrzeit sowie Enddatum und -uhrzeit anzeigen.

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources      : {Don, Betty, Bobby, Sally}
ClonedResources      : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

## Überwachen von PostgreSQL-Klonvorgängen

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**.

## 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 Datenbank Anwendungen | Wählen Sie <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme          | Wählen Sie <b>Pfad</b> 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"](#)

## Löschen oder Aufteilen von PostgreSQL-Cluster-Klonen nach dem Upgrade von SnapCenter

Nach dem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource aufteilen, aus der die Klone erstellt wurden.

### Informationen zu diesem Vorgang

Wenn Sie den Speicherbedarf der versteckten Klone ermitteln möchten, führen Sie den folgenden Befehl aus:  
`Get-SmClone -ListStorageFootprint`

### Schritte

1. Löschen Sie die Sicherungen der geklonten Ressourcen mithilfe des Cmdlets „remove-smbbackup“.
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mithilfe des Cmdlets „remove-smresourcegroup“.
3. Entfernen Sie den Schutz der geklonten Ressource mithilfe des Cmdlets „remove-smprotectresource“.
4. Wählen Sie die übergeordnete Ressource auf der Seite „Ressourcen“ aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht „Kopien verwalten“ die Klone entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
6. Wählen Sie die Klone aus und klicken Sie dann auf , um Klone zu löschen, oder klicken Sie auf  um die Klone zu teilen.
7. Klicken Sie auf **OK**.

# MySQL schützen

## SnapCenter -Plug-in für MySQL

### Übersicht über das SnapCenter -Plug-in für MySQL

Das SnapCenter -Plug-in für MySQL-Datenbanken ist eine hostseitige Komponente der NetApp SnapCenter software , die eine anwendungsbewusste Datenschutzverwaltung von MySQL-Datenbanken ermöglicht. Das Plug-in für MySQL-Datenbanken automatisiert die Sicherung, Wiederherstellung und das Klonen von MySQL-Datenbanken in Ihrer SnapCenter Umgebung.

SnapCenter unterstützt MySQL-Setups mit einer Instanz. Sie können das Plug-in für MySQL-Datenbanken sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird MySQL als manuelle Ressource unterstützt.

Wenn das Plug-in für MySQL-Datenbanken installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen. Sie können das Plug-in auch mit der NetApp SnapVault -Technologie verwenden, um eine Disk-to-Disk-Backup-Replikation zur Einhaltung von Standards durchzuführen.

Das SnapCenter -Plug-in für MySQL unterstützt NFS und SAN auf ONTAP und Azure NetApp Dateispeicherlayouts.

Das virtuelle Speicherlayout VMDK, vVol und RDM wird unterstützt.

Symbolische Links werden nicht unterstützt.

### Was Sie mit dem SnapCenter Plug-in für MySQL tun können

Wenn Sie das Plug-in für MySQL-Datenbanken in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von MySQL-Instanzen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Instanzen hinzufügen.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

### SnapCenter Plug-in für MySQL-Funktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit dem Plug-in für MySQL-Datenbanken zu arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter .

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Kopiertechnologie**

SnapCenter verwendet die Snapshot-Technologie von NetApp mit dem Plug-in für MySQL-Datenbanken zum Sichern von Ressourcen.

Die Verwendung des Plug-ins für MySQL bietet außerdem die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung für die Consistency Group (CG)-Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Unterstützung für Linux LVM auf dem XFS-Dateisystem.

## **Vom SnapCenter Plug-in für MySQL unterstützte Speichertypen**

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen Maschinen als auch auf virtuellen Maschinen (VMs). Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter -Plug-in für MySQL installieren.

| Maschine          | Speichertyp                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physischer Server | <ul style="list-style-type: none"> <li>• FC-verbundene LUNs</li> <li>• Über iSCSI verbundene LUNs</li> <li>• Über NFS verbundene Volumes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| VMware ESXi       | <ul style="list-style-type: none"> <li>• RDM-LUNs, die über einen FC oder iSCSI ESXi HBA verbunden sind. Das Scannen von Host-Bus-Adaptoren (HBAs) kann lange dauern, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt.</li> </ul> <p>Sie können die Datei <b>LinuxConfig.pm</b> unter <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> bearbeiten, um den Wert des Parameters <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> auf 1 zu setzen und nur die HBAs erneut zu scannen, die in HBA_DRIVER_NAMES aufgeführt sind.</p> <ul style="list-style-type: none"> <li>• iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind</li> <li>• VMDKs auf NFS-Datenspeichern</li> <li>• VMDKs auf VMFS erstellt</li> <li>• NFS-Volumes, die direkt mit dem Gastsystem verbunden sind</li> <li>• vVol-Datenspeicher auf NFS und SAN</li> </ul> <p>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p> |

## Für das MySQL-Plug-In erforderliche Mindest ONTAP Berechtigungen

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN erstellen
  - LUN erstellen
  - LUN löschen

- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- LUN-Igroup umbenennen
- lun igroup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN persistent-reservation clear
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen

- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot-Modify-Snaplock-Ablaufzeit
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle anzeigen



## Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation für MySQL

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#).

## Backup-Strategie für MySQL

### Definieren Sie eine Sicherungsstrategie für MySQL

Durch die Definition einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge verfügen Sie über die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

### Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

### Schritte

1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.
4. Entscheiden Sie, ob Sie eine auf Snapshot-Kopien basierende Richtlinie erstellen möchten, um anwendungskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
6. Bestimmen Sie die Aufbewahrungsdauer für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
7. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

### **Automatische Erkennung von Ressourcen auf Linux-Hosts**

Ressourcen sind MySQL-Instanzen auf dem Linux-Host, die von SnapCenter verwaltet werden. Nach der Installation des SnapCenter -Plug-ins für MySQL werden die MySQL-Instanzen auf diesem Linux-Host automatisch erkannt und auf der Ressourcenseite angezeigt.

### **Unterstützte Sicherungstypen**

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot-Kopien basierenden Sicherungstyp für MySQL-Datenbanken.

### **Snapshot-Kopie-basierte Sicherung**

Auf Snapshot-Kopien basierende Backups nutzen die Snapshot-Technologie von NetApp , um schreibgeschützte Online-Kopien der Volumes zu erstellen, auf denen sich die MySQL-Datenbanken befinden.

### **So verwendet das SnapCenter Plug-in für MySQL Konsistenzgruppen-Snapshots**

Sie können das Plug-In verwenden, um Konsistenzgruppen-Snapshots für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes aufnehmen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe besteht aus gleichzeitigen Snapshots mehrerer Volumes und bietet konsistente Kopien einer Volumengruppe.

Sie können auch die Wartezeit angeben, die der Speichercontroller benötigt, um Snapshots konsistent zu gruppieren. Die verfügbaren Wartezeitoptionen sind **Dringend**, **Mittel** und **Entspannt**. Sie können die WAFL-Synchronisierung (Write Anywhere File Layout) auch während des konsistenten Gruppen-Snapshot-Vorgangs aktivieren oder deaktivieren. Die WAFL Synchronisierung verbessert die Leistung eines Konsistenzgruppen-Snapshots.

### **So verwaltet SnapCenter die Verwaltung von Protokollsicherungen**

SnapCenter verwaltet die Datensicherungen auf Speichersystem- und Dateisystemebene.

## Überlegungen zur Festlegung von Sicherungszeitplänen für MySQL

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen)

Die Sicherungshäufigkeit, bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen)

Sicherungszeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird.

## Anzahl der für MySQL benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

## Sicherungsnamenskonventionen für Plug-in für MySQL-Datenbanken

Sie können entweder die standardmäßige Snapshot-Benennungskonvention oder eine benutzerdefinierte Benennungskonvention verwenden. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standardbenennungskonvention:

`resourcegroupname_hostname_timestamp`

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- *dts1* ist der Name der Ressourcengruppe.
- *mach1x88* ist der Hostname.
- *03-12-2015\_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Snapshot-Namensformat beim Schützen von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: customtext\_resourcegroup\_policy\_hostname oder resourcegroup\_hostname. Standardmäßig wird dem Snapshot-Namen das Zeitstempel-Suffix hinzugefügt.

## Wiederherstellungs- und Recovery-Strategie für MySQL

### Definieren Sie eine Wiederherstellungsstrategie für MySQL-Ressourcen

Sie müssen vor der Wiederherstellung Ihrer Datenbank eine Strategie definieren, damit Sie Wiederherstellungsvorgänge erfolgreich durchführen können.



Es wird nur die manuelle Wiederherstellung der Datenbank unterstützt.

#### Schritte

1. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für manuell hinzugefügte MySQL-Ressourcen
2. Ermitteln Sie die unterstützten Wiederherstellungsstrategien für automatisch erkannte MySQL-Datenbanken
3. Entscheiden Sie sich für die Art der Wiederherstellungsvorgänge, die Sie durchführen möchten.

### Unterstützte Wiederherstellungsstrategien für manuell hinzugefügte MySQL-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte MySQL-Ressourcen.



Sie können manuell hinzugefügte MySQL-Ressourcen nicht wiederherstellen.

### Vollständige Ressourcenwiederherstellung

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem für die Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

### Art der unterstützten Wiederherstellungsstrategie für automatisch erkanntes MySQL

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können.

Die vollständige Ressourcenwiederherstellung ist die unterstützte Wiederherstellungsstrategie für automatisch erkannte MySQL-Datenbanken. Dadurch werden alle Volumes, Qtrees und LUNs einer Ressource wiederhergestellt.

### Arten von Wiederherstellungsvorgängen für automatisch erkanntes MySQL

Das SnapCenter -Plug-in für MySQL unterstützt Single File SnapRestore und Connect-

and-Copy-Wiederherstellungstypen für automatisch erkannte MySQL-Datenbanken.

Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das ausgewählte Backup von einem SnapMirror oder SnapVault Sekundärspeicherort stammt und die Option **Complete Resource** ausgewählt ist

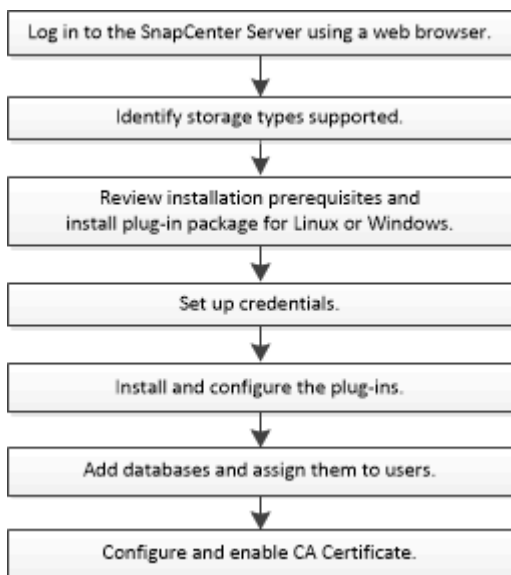
Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien durchgeführt:

- Wenn nur die Option **Komplette Ressource** ausgewählt ist
- Wenn das Backup von einem SnapMirror oder SnapVault Sekundärspeicherort ausgewählt wird und die Option **Complete Resource** ausgewählt ist

## Vorbereiten der Installation des SnapCenter -Plug-ins für MySQL

### Installationsablauf des SnapCenter Plug-ins für MySQL

Sie sollten das SnapCenter -Plug-in für MySQL installieren und einrichten, wenn Sie MySQL-Datenbanken schützen möchten.



### Voraussetzungen zum Hinzufügen von Hosts und Installieren des SnapCenter -Plug-ins für MySQL

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Das SnapCenter Plug-in für MySQL ist sowohl in Windows- als auch in Linux-Umgebungen verfügbar.

- Sie müssen Java 11 auf Ihrem Host installiert haben.



IBM Java wird auf Windows- und Linux-Hosts nicht unterstützt.

- Unter Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „LocalSystem“ ausgeführt werden. Dies ist das Standardverhalten, wenn das Plug-in für MySQL als Domänenadministrator installiert wird.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren. Das SnapCenter -Plug-in für Microsoft Windows wird standardmäßig mit dem MySQL-Plug-in auf Windows-Hosts bereitgestellt.
- Der SnapCenter -Server sollte Zugriff auf den 8145- oder benutzerdefinierten Port des Plug-ins für den MySQL-Host haben.
- Für MySQL 5.7 sollte Binlog in der MySQL-Konfigurationsdatei (my.cnf oder mysql-server.cnf) angegeben werden.

## Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Während der Installation des Plug-ins für MySQL auf einem Windows-Host wird das SnapCenter Plug-in für Microsoft Windows automatisch installiert.
- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Windows-Host installiert haben.

["Laden Sie JAVA für alle Betriebssysteme herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

## Linux-Hosts

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

["Laden Sie JAVA für alle Betriebssysteme herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Bei MySQL-Datenbanken, die auf einem Linux-Host ausgeführt werden, wird bei der Installation des Plug-ins für MySQL automatisch das SnapCenter Plug-in für UNIX installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

## Ergänzende Befehle

Um einen zusätzlichen Befehl im SnapCenter -Plug-in für MySQL auszuführen, müssen Sie ihn in die Datei *allowed\_commands.config* aufnehmen.

- Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed\_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/ NetApp/ snapcenter/ scc/ etc/ allowed\_commands.config*

Um zusätzliche Befehle auf dem Plug-In-Host zuzulassen, öffnen Sie die Datei *allowed\_commands.config* in einem Editor. Geben Sie jeden Befehl in einer separaten Zeile ein. Bei den Befehlen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen

angeben und den Pfadnamen in Anführungszeichen (") einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: mount Befehl: umount Befehl: "C:\Programme\ NetApp\SnapCreator commands\sdcli.exe" Befehl: myscript.bat

Wenn die Datei *allowed\_commands.config* nicht vorhanden ist, werden die Befehle oder die Skriptausführung blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."

Wenn der Befehl oder das Skript nicht in der Datei „*allowed\_commands.config*“ vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit dem folgenden Fehler fehl:

"[/mnt/mount -a] Ausführung nicht erlaubt. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen."



Um alle Befehle zuzulassen, sollten Sie keinen Platzhaltereintrag (\*) verwenden.

## Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den Linux-Host

SnapCenter ermöglicht einem Nicht-Root-Benutzer, das SnapCenter -Plug-In-Paket für Linux zu installieren und den Plug-In-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

### Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Wenn die Umask 0027 ist, stellen Sie sicher, dass der Java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben. Andernfalls kann die Plug-in-Installation fehlschlagen.
- Stellen Sie beim Nicht-Root-Benutzer sicher, dass der Name des Nicht-Root-Benutzers und der Benutzergruppe identisch sind.
- Bearbeiten Sie die Datei */etc/ssh/sshd\_config*, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- /home/*LINUX\_USER*/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/bin/spl

## Schritte

1. Melden Sie sich beim Linux-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für Linux installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.



```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei `/etc/sudoers` hinzufügen: „/`<crs_home>`/bin/olsnodes“

Sie können den Wert von `crs_home` aus der Datei `/etc/oracle/olr.loc` abrufen.

`LINUX_USER` ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei `sc_unix_plugins_checksum.txt` abrufen, die sich hier befindet:

- `_C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` \_ wenn SnapCenter Server auf einem Windows-Host installiert ist.
- `_/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` \_ wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <p>Microsoft Windows</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                                                                                                                                                                        |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <p>5 GB</p> <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p>                                                                                                                                                                                           |

## Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux

Bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren, sollten Sie mit einigen grundlegenden Anforderungen an Speicherplatz und Größe des Hostsystems vertraut sein.

| Artikel         | Anforderungen                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | 2 GB <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | <p>Java 11 Oracle Java und OpenJDK</p> <p>Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a>.</p>                                                           |

## Einrichten der Anmeldeinformationen für das SnapCenter -Plug-in für MySQL

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Datenbanken oder Windows-Dateisystemen erstellen.

### Informationen zu diesem Vorgang

- Linux-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldeinformationen für den Root-Benutzer oder für einen Nicht-Root-Benutzer mit Sudo-Berechtigungen einrichten, um den Plug-In-Prozess zu installieren und zu starten.

**Best Practice:** Obwohl Sie Anmeldeinformationen für Linux erstellen dürfen, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

- Windows-Hosts

Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.

Sie müssen die Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die zum Konfigurieren der Anmeldeinformationen erforderlichen Informationen an:

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |

| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername                      | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i></p> <p>Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (&lt;) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als &lt;!10, kleiner als 10 &lt;!, Backtick `12.</p> |
| Passwort                          | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Authentifizierungsmodus           | Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen <b>Sudo-Berechtigungen verwenden</b>, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p> <div>  <p>Gilt nur für Linux-Benutzer.</p> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

## Installieren Sie das SnapCenter -Plug-in für MySQL

### Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert. Sie können den Host hinzufügen und Plug-In-Pakete für einen einzelnen Host installieren.

#### Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zur Verwaltung von Hosts.

#### Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.

#### 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              | <p>Wählen Sie den Hosttyp aus:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> </ul> <div>  <p>Das Plug-in für MySQL muss auf dem MySQL-Datenbankserver installiert werden.</p> </div>                                                                                                                                                                                                                                                                                                                                                                                                               |
| Hostname             | <p>Geben Sie den Hostnamen für die Kommunikation ein. Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Anmeldeinformationen | <p>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.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div>  <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

Wenn Sie die REST-API zum Installieren des Plug-ins für MySQL verwenden, müssen Sie die Version als 3.0 übergeben. Beispiel: MySQL:3.0

6. (Optional) Klicken Sie auf **Weitere Optionen**.

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen                                                                                       | <p>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.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |
| Installationspfad                                                                           | <p>Das Plug-in für MySQL wird auf dem MySQL-Client-Host installiert und dieser Host kann entweder ein Windows- oder ein Linux-System sein.</p> <ul style="list-style-type: none"> <li>• Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter. Optional können Sie den Pfad anpassen.</li> <li>• Für das SnapCenter Plug-ins-Paket für Linux ist der Standardpfad /opt/ NetApp/snapcenter. Optional können Sie den Pfad anpassen.</li> </ul>                                                     |
| Vorinstallationsprüfungen überspringen                                                      | 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.                                                                                                                                                                                                                                                                                                                                        |
| Alle Hosts im Cluster hinzufügen                                                            | Nicht zutreffend.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | Nicht zutreffend.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-Ins) und Java-Version (für Linux-Plug-Ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, 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, müssen Sie das Problem beheben.





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

8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.



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

9. Überwachen Sie den Installationsfortschritt.

- Für Windows-Plug-Ins befinden sich die Installations- und Upgrade-Protokolle unter: `C:\Windows\SnapCenter plugin\Install<JOBID>\_`
- Für Linux-Plug-Ins befinden sich die Installationsprotokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_` und die Upgrade-Protokolle unter: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

### Nach Abschluss

Wenn Sie auf die SnapCenter Version 6.0 aktualisieren möchten, wird das vorhandene PERL-basierte Plug-in für MySQL vom Remote-Plug-in-Server deinstalliert.

### Installieren Sie SnapCenter Plug-in-Pakete für Linux oder Windows auf mehreren Remote-Hosts mithilfe von Cmdlets

Sie können die SnapCenter -Plug-in-Pakete für Linux oder Windows mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

### Bevor Sie beginnen

Sie müssen sich auf jedem Host, auf dem Sie das Plug-In-Paket installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-In auf mehreren Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

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](#) .

Sie können die Option `-skippercheck` verwenden, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

## Installieren Sie das SnapCenter -Plug-in für MySQL auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle

Sie sollten das SnapCenter Plug-in für MySQL-Datenbanken mithilfe der SnapCenter Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie das Plug-In für MySQL-Datenbanken entweder im Konsolenmodus oder im Hintergrundmodus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

### Bevor Sie beginnen

- Sie sollten das Plug-in für MySQL-Datenbanken auf jedem Linux-Host installieren, auf dem die MySQL-Instanz geschützt werden muss.
- Der Linux-Host, auf dem Sie das SnapCenter -Plug-in für MySQL-Datenbanken installieren, muss die abhängigen Software-, Datenbank- und Betriebssystemanforderungen erfüllen.

Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den unterstützten Konfigurationen.

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Das SnapCenter -Plug-in für MySQL-Datenbanken ist Teil des SnapCenter -Plug-in-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins-Paket für Linux installieren, sollten Sie SnapCenter bereits auf einem Windows-Host installiert haben.

### Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter Plug-ins-Pakets für Linux (snapcenter\_linux\_host\_plugin.bin) von C:\ProgramData\NetApp\ SnapCenter\Package Repository auf den Host, auf dem Sie das Plug-in für MySQL installieren möchten.

Sie können auf diesen Pfad von dem Host aus zugreifen, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei kopiert haben.
3. Installieren Sie das Plug-In:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT gibt den SMCore HTTPS-Kommunikationsport an.
- -DSERVER\_IP gibt die IP-Adresse des SnapCenter -Servers an.
- -DSERVER\_HTTPS\_PORT gibt den HTTPS-Port des SnapCenter -Servers an.
- -DUSER\_INSTALL\_DIR gibt das Verzeichnis an, in dem Sie das SnapCenter Plug-Ins-Paket für Linux installieren möchten.
- DINSTALL\_LOG\_NAME gibt den Namen der Protokolldatei an.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Bearbeiten Sie die Datei `/<Installationsverzeichnis>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties` und fügen Sie dann den Parameter `PLUGINS_ENABLED = MySQL:3.0` hinzu.
5. Fügen Sie den Host mit dem Cmdlet `Add-Smhost` und den erforderlichen Parametern zum SnapCenter-Server hinzu.

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 ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Überwachen Sie den Status der Installation des Plug-ins für MySQL

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

### CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

#### Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

### Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

#### Schritte

1. Führen Sie auf der GUI Folgendes aus:

- Doppelklicken Sie auf das Zertifikat.
- Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
- Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
- Kopieren Sie die Hexadezimalzeichen aus dem Feld.
- Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:

- Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

*Get-ChildItem -Pfad Zertifikat:\LocalMachine\My*

- Kopieren Sie den Fingerabdruck.

## Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-In-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## Konfigurieren Sie das CA-Zertifikat für den SnapCenter MySQL Plug-Ins-Dienst auf dem Linux-Host

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

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter `/opt/NetApp/snapcenter/scc/etc` befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Dies ist der Wert, der dem Schlüssel „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_in_cert" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE\_PASS in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: /opt/NetApp/snapcenter/scc/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder  
Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/ NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE\_PASS in der Datei agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei agent.properties.

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC\_CERTIFICATE\_ALIAS.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

## Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

### Informationen zu diesem Vorgang



- SnapCenter Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist „opt/NetApp/snapcenter/scc/etc/crl“.

### Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* anhand des Schlüssels *CRL\_PATH* ändern und aktualisieren.

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

## Konfigurieren Sie das CA-Zertifikat für den SnapCenter MySQL Plug-Ins-Dienst auf dem Windows-Host

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

Die Plug-ins verwenden die Datei *keystore.jks*, die sich unter *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Es handelt sich um den Wert, der dem Schlüssel *KEYSTORE\_PASS* entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

```
C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

```
keytool -keypasswd -alias "Aliasname_im_Zertifikat" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel *KEYSTORE\_PASS* in der Datei *agent.properties*.

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



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

## Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels `KEYSTORE_PASS` in der Datei `agent.properties`.

```
keytool -keypasswd -alias "Aliasname_im_CA_Zertifikat" -keystore keystore.jks
```

8. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei *agent.properties*.

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC\_CERTIFICATE\_ALIAS.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter -Plug-Ins

#### Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe ["So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat"](#).
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist 'C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\crl'.

#### Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* anhand des Schlüssels 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.

## Bereiten Sie sich auf den Datenschutz vor

### Voraussetzungen für die Verwendung des SnapCenter -Plug-ins für MySQL

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

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich beim SnapCenter -Server an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen und gegebenenfalls Anmeldeinformationen erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

Sie müssen den Java-Pfad in der Umgebungspfadvariable des Hostcomputers festlegen.

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.

### So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von MySQL verwendet

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei Ressourcen handelt es sich normalerweise um MySQL-Instanzen, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Sicherungshäufigkeit, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe

aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

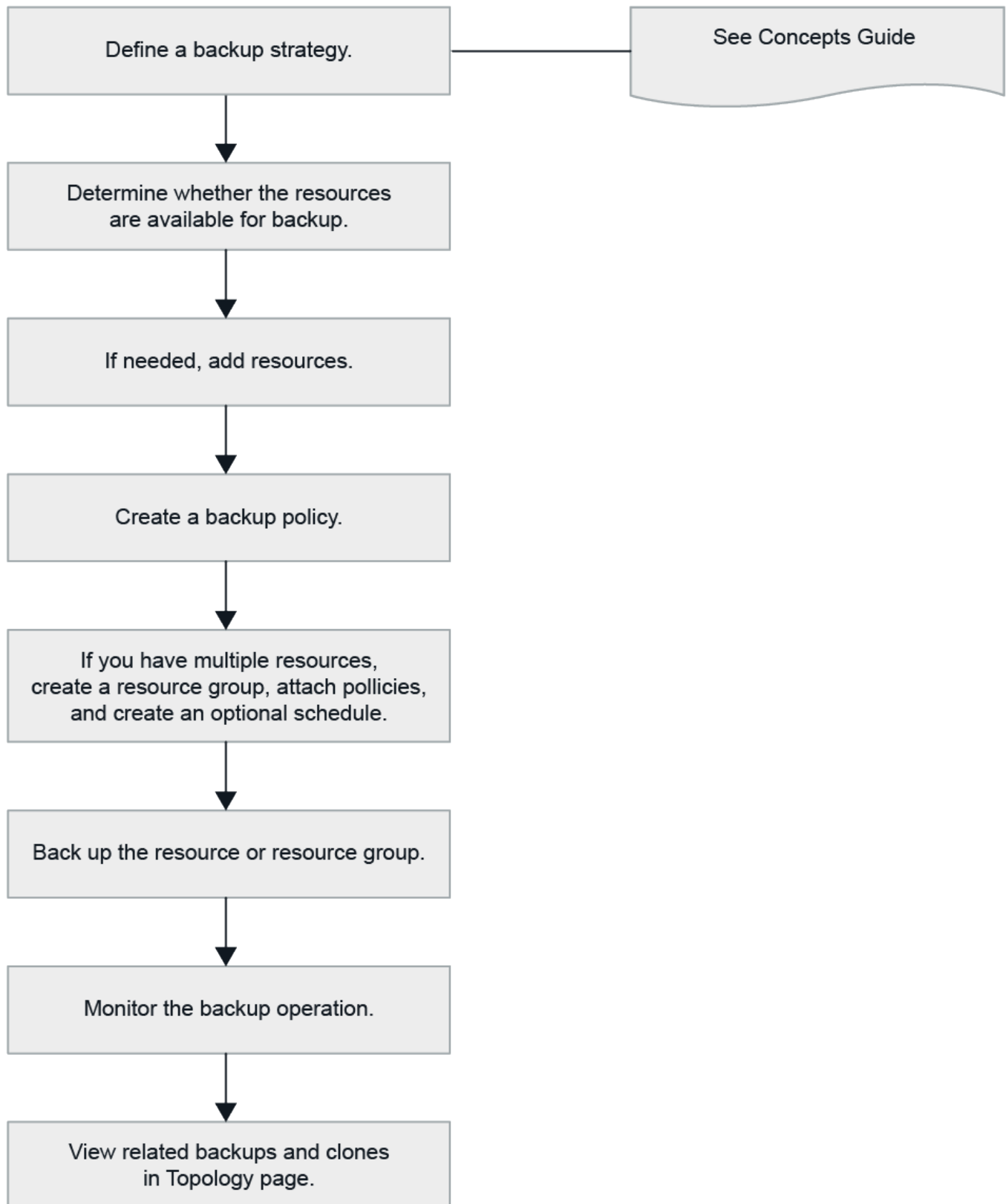
Stellen Sie sich eine Ressourcengruppe so vor, dass sie definiert, was Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als ob sie definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken im Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine vollständige Sicherung durchgeführt wird.

## **Sichern von MySQL-Ressourcen**

### **Sichern von MySQL-Ressourcen**

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Sicherungsworkflow umfasst die Planung, die Identifizierung der zu sichernden Datenbanken, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets. ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Automatisches Erkennen der Datenbanken

Ressourcen sind MySQL-Datenbanken auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren MySQL-Datenbanken ermittelt haben.

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen abgeschlossen haben.
- Das SnapCenter -Plug-in für MySQL unterstützt keine automatische Erkennung der Ressourcen, die sich in virtuellen RDM/VMDK-Umgebungen befinden. Sie müssen die Speicherinformationen für virtuelle Umgebungen angeben, während Sie die Datenbanken manuell hinzufügen.

### Informationen zu diesem Vorgang

- Nach der Installation des Plug-ins werden alle Datenbanken auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.
- Nur Datenbanken werden automatisch erkannt.

Die automatisch erkannten Ressourcen können nicht geändert oder gelöscht werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für MySQL aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste „Anzeigen“ aus.
3. (Optional) Klicken Sie auf  \* und wählen Sie dann den Hostnamen aus.

Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen anzuzeigen.

Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp -Speichersystem befindet und geschützt ist und kein Sicherungsvorgang ausgeführt wird, wird in der Spalte „Gesamtstatus“ die Meldung „Sicherung nicht ausgeführt“ angezeigt. Andernfalls ändert sich der Status basierend auf dem letzten Sicherungsstatus in „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“.



Sie müssen die Ressourcen aktualisieren, wenn die Instanzen außerhalb von SnapCenter umbenannt werden.

## Ressourcen manuell zum Plug-In-Host hinzufügen

Die automatische Erkennung wird auf Windows-Hosts nicht unterstützt. Sie müssen MySQL-Instanzen und Datenbankressourcen manuell hinzufügen.

### Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten von Speichersystemverbindungen abgeschlossen haben.

## Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter -Plug-in für MySQL aus der Dropdown-Liste aus und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite „Ressourcen“ auf **MySQL-Ressourcen hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Name                 | Geben Sie den Datenbanknamen an.                                                                                                  |
| Hostname             | Geben Sie den Hostnamen ein.                                                                                                      |
| Typ                  | Instanz auswählen.                                                                                                                |
| Beispiel             | Nicht zutreffend.                                                                                                                 |
| Anmeldeinformationen | Wählen Sie die Anmeldeinformationen aus oder fügen Sie Informationen zu den Anmeldeinformationen hinzu.<br><br>Dies ist optional. |

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ einen Speichertyp und ein oder mehrere Volumes, LUNs und Qtrees aus und klicken Sie dann auf **Speichern**.

Optional: Sie können auf das \* klicken  \* Symbol zum Hinzufügen weiterer Volumes, LUNs und Qtrees aus anderen Speichersystemen.

5. Optional: Geben Sie auf der Seite „Ressourceneinstellungen“ benutzerdefinierte Schlüssel-Wert-Paare für das MySQL-Plug-In ein.
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Die Datenbanken werden zusammen mit Informationen wie dem Hostnamen, den zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie die Ressourcen den Benutzern zuweisen. Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

["Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"](#)

Nachdem Sie die Datenbanken hinzugefügt haben, können Sie die MySQL-Datenbankdetails ändern.

## Erstellen von Sicherungsrichtlinien für MySQL

Bevor Sie SnapCenter zum Sichern von MySQL-Ressourcen verwenden, müssen Sie



eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren.

### Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für MySQL-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen von Ressourcen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

Darüber hinaus können Sie in der Richtlinie Replikations-, Skript- und Anwendungseinstellungen angeben. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

### 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. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie den Speichertyp aus.
  - b. Geben Sie im Abschnitt „Benutzerdefinierte Sicherungseinstellungen“ alle spezifischen Sicherungseinstellungen an, die im Schlüssel-Wert-Format an das Plug-In übergeben werden müssen.  
  
Sie können mehrere Schlüsselwerte angeben, die an das Plug-In übergeben werden sollen.
6. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:
  - a. Geben Sie den Zeitplantyp an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- a. Geben Sie im Abschnitt „Snapshot-Einstellungen“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

| Wenn Sie wollen...                                                 | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Snapshots                   | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> <div><p>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.</p></div> <div><p>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.</p></div> |
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Wenn Sie wollen...                | Dann...                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sperrzeitraum für Snapshot-Kopien | <p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopien</b> und geben Sie Tage, Monate oder Jahre an.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p> |

b. Wählen Sie eine 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.

7. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b> | <p>Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation).</p> <p>Wenn die Schutzbeziehung in ONTAP vom Typ „Mirror und Vault“ ist und Sie nur diese Option auswählen, wird der auf dem primären Server erstellte Snapshot nicht zum Ziel übertragen, sondern im Ziel aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird die folgende Fehlermeldung angezeigt: „Der sekundäre Speicherort ist für die ausgewählte gewölbte/gespiegelte Sicherung nicht verfügbar.“</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen von MySQL-Ressourcen-bezogenen Sicherungen und Klonen auf der Seite „Topologie“"</a> .</p> |

| Für dieses Feld...                                                                         | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b> | <p>Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.</p> <p>Weitere Informationen zu SnapLock Vault finden Sie unter Commit Snapshots to WORM on a vault destination</p> <p>Sehen "<a href="#">Anzeigen von MySQL-Ressourcen-bezogenen Sicherungen und Klonen auf der Seite „Topologie“</a>" .</p> |
| <b>Fehler bei der Wiederholungsanzahl</b>                                                  | Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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

## Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### Informationen zu diesem Vorgang

- 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 Klonen nach Ablauf des SnapLock manuell bereinigen.

## 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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | <p>Geben Sie einen Namen für die Ressourcengruppe ein.</p> <div><p>Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</p></div>                                                                                                     |
| Schlagwörter                                                  | <p>Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.</p> <p>Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.</p>                                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | <p>Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.</p> <p>Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p> |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

Dies hilft, Informationen auf dem Bildschirm zu filtern.

5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:
  - a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                             | Machen Sie Folgendes...                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Snapshot-Vorgangs der Konsistenzgruppe zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs anzugeben.<br><br>Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                            | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

+

- Klicken Sie auf den Pfeil **Skripts** 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.
- Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

| Parameter         | Einstellung | Beschreibung                                                              |
|-------------------|-------------|---------------------------------------------------------------------------|
| ARCHIV_LOG_ENABLE | (J/N)       | Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle. |

| Parameter                     | Einstellung                | Beschreibung                                                                                                                                                                                                                                                 |
|-------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIV_LOG_RETENTION          | Anzahl_der_Tage            | Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden.<br><br>Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein.                                                                                             |
| ARCHIVE_LOG_DIR               | change_info_directory/logs | Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.                                                                                                                                                                                          |
| ARCHIVE_LOG_EXT               | Dateierweiterung           | Gibt die Erweiterungslänge der Archivprotokolldatei an.<br><br>Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.1615185519429 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (J/N)                      | Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen.<br><br>Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.                                                                       |



Die benutzerdefinierten Schlüssel-Wert-Paare werden für MySQL Linux-Plug-in-Systeme unterstützt, nicht jedoch für MySQL-Datenbanken, die als zentrales Windows-Plug-in registriert sind.

- c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                                                                        | Dann...                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar. | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*. |

| Falls Sie es wollen...                                                                              | Dann...                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                          | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                                                                     |
| Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot-Kopien zu erstellen. | Wählen Sie <b>Andere</b> aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen. |

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

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



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

Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

- b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \* \* für die Richtlinie, die Sie konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist „policy\_name“ 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. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für MySQL-Ressourcen 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                  |
|------------------------------------------------------|----------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> . |

| Wenn Sie wollen...          | Machen Sie Folgendes...                                                                                         |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| Planen Sie eine Überprüfung | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für MySQL

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern, Wiederherstellen oder Klonen von MySQL-Datenbanken verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

### Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

Dieses Beispiel zeigt, wie Sie mit Windows-Anmeldeinformationen neue Anmeldeinformationen mit dem Namen „FinanceAdmin“ erstellen:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. Fügen Sie den MySQL-Kommunikationshost zum SnapCenter -Server hinzu.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode mysql
```

5. Installieren Sie das Paket und das SnapCenter -Plug-in für MySQL auf dem Host.

Für Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
mysql
```

Für Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql  
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. Legen Sie den Pfad zur SQLLIB fest.

Für Windows verwendet das MySQL-Plug-In den Standardpfad für den SQLLIB-Ordner:  
„C:\Programme\IBM\SQLLIB\BIN“.

Wenn Sie den Standardpfad überschreiben möchten, verwenden Sie den folgenden Befehl.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{ "MySQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN" }
```

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"](#) .

## MySQL sichern

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Stellen Sie bei Sicherungsvorgängen auf Basis von Snapshot-Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Bei Pre- und Post-Befehlen für Quiesce-, Snapshot- und Unquiesce-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Wählen \*\* und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- Wählen Sie den Pfeil **Backups** aus, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                            | Machen Sie Folgendes...                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Vorgangs „Consistency Group Snapshot“ zu warten | Wählen Sie <b>Dringend</b> , <b>Mittel</b> oder <b>Entspannt</b> aus, um die Wartezeit für die Fertigstellung des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden. |
| WAFL -Synchronisierung deaktivieren                                                           | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                                      |

- Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.

Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

- Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                   | Dann...                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                               | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                      |
| SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.                                       |
| So geben Sie den Befehl zum Erstellen eines Snapshots ein                                                                                                | Wählen Sie <b>Andere</b> und geben Sie dann den Befehl zum Erstellen eines Snapshots ein. |

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

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



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

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

- b. Wählen \* \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

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

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Wählen Sie **Jetzt sichern**.

10. 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. Wählen Sie **Backup**.

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

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl.

Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript startet der Befehl `do_start method` den SnapCenter VMware-Plug-in-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseUrl  
https:\\snapctr.demo.netapp.com:8146\\
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Fügen Sie mithilfe des Cmdlets `Add-SmResources` manuelle Ressourcen hinzu.

Dieses Beispiel zeigt, wie eine MySQL-Instanz hinzugefügt wird:



```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.
4. Schützen Sie die Ressource oder fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.
5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert wird:

```
C:\PS> New-SmBackup -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
luginName"="MySQL"} -Policy "MySQL_snapshotbased"
```

In diesem Beispiel wird eine geschützte Ressource gesichert:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy mysql_policy2
```

6. Überwachen Sie den Auftragsstatus (wird ausgeführt, abgeschlossen oder fehlgeschlagen) mithilfe des Cmdlets Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Überwachen Sie die Details des Sicherungsauftrags wie Sicherungs-ID und Sicherungsname, um mithilfe des Cmdlets Get-SmBackupReport Wiederherstellungs- oder Klonvorgänge durchzuführen.

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses       :
ReportDataCreatedDateTime :

```

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"](#) .

## Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

### Informationen zu diesem Vorgang

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie  und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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. Wählen Sie **Backup**.

5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Überwachen von MySQL-Sicherungsvorgängen

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 Sie Datenschutzvorgänge auf MySQL-Instanzen 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.

## Abbrechen von Sicherungsvorgängen für MySQL

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.

- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

## Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <ol style="list-style-type: none"> <li>a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</li> <li>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b>.</li> </ol>                                                                                                                                                                         |
| Aktivitätsbereich | <ol style="list-style-type: none"> <li>a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</li> <li>b. Wählen Sie den Vorgang aus.</li> <li>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</li> </ol> |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## MySQL-Backups und -Klone auf der Topologieseite anzeigen

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

### Informationen zu diesem Vorgang

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.

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

### 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 **Zusammenfassungskarte**, um eine Zusammenfassung der Anzahl der auf dem primären und sekundären Speicher verfügbaren Backups und Klone anzuzeigen.

Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Klone an.

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 die Anwendungsressource auf 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.

Nach der On-Demand-Sicherung werden durch Klicken auf die Schaltfläche **Aktualisieren** die Details der Sicherung oder des Klons aktualisiert.

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.

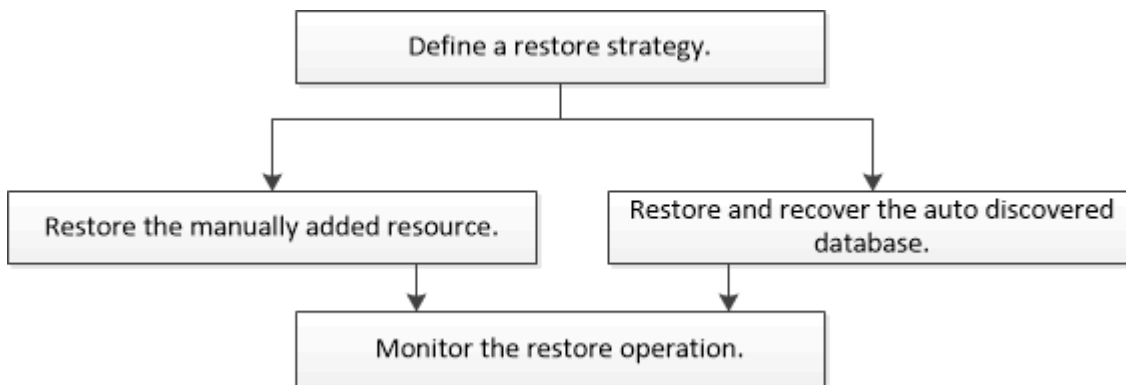
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

## MySQL wiederherstellen

### Wiederherstellungs-Workflow

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

### Wiederherstellen und Wiederherstellen einer manuell hinzugefügten Ressourcensicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

#### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:

- Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed\_commands.config*
- Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed\_commands.config*



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

#### Informationen zu diesem Vorgang

- Bei ONTAP 9.12.1 und früheren 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.



## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                           |                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| search                                      |                        |
| Backup Name                                 | End Date                                                                                                  |
| rg1_scpr0191685001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option **Vollständige Ressource** aus.

- a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumes der MySQL-Datenbank wiederhergestellt.

Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

Sie können mehrere LUNs auswählen.



Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, Qtrees oder LUNs wiederhergestellt.

7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Befehle zum Aufheben der Bereitstellung verfügbar.

8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle verfügbar.

9. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

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

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime | BackupType |
|----------|-------------------------------|------------|------------|
| -----    | -----                         | -----      | -----      |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:02:32   |
| AM       | Full Backup                   |            |            |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:23:17   |
| AM       |                               |            |            |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :

```

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"](#) .

## Wiederherstellen und Wiederherstellen einer automatisch erkannten Datenbanksicherung

Sie können SnapCenter verwenden, um Daten aus einem oder mehreren Backups wiederherzustellen.

### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.
- Bei Befehlen vor und nach der Wiederherstellung sowie zum Einhängen und Aufheben der Einhängung

sollten Sie prüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:

- Standardspeicherort auf dem Windows-Host: `C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Standardspeicherort auf dem Linux-Host: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

### Informationen zu diesem Vorgang

- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Die automatische Wiederherstellung zu einem bestimmten Zeitpunkt und auf die Minute genau wird nicht unterstützt.
- 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 **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.

5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.

| Primary Backup(s)                            |                                                                                                           |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| search                                       |                        |
| Backup Name                                  | End Date                                                                                                  |
| rg1_scscr0191683001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ **Vollständige Ressource** aus, um die konfigurierten Datenvolumes der MySQL-Datenbank wiederherzustellen.
7. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Befehle zum Aufheben der Bereitstellung verfügbar.

8. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

Für automatisch erkannte Ressourcen sind keine Mount-Befehle verfügbar.

9. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets

Das Wiederherstellen einer Ressourcensicherung umfasst das Einleiten einer Verbindungssitzung mit dem SnapCenter -Server, das Auflisten der Sicherungen und Abrufen von Sicherungsinformationen sowie das Wiederherstellen einer Sicherung.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

### Schritte

1. Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „`Get-SmBackup`“ und „`Get-SmBackupReport`“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId    | BackupName                             | BackupTime  |
|-------------|----------------------------------------|-------------|
| BackupType  |                                        |             |
| -----       | -----                                  | -----       |
| -----       |                                        |             |
| 1           | Payroll Dataset_vise-f6_08... 8/4/2015 | 11:02:32 AM |
| Full Backup |                                        |             |
| 2           | Payroll Dataset_vise-f6_08... 8/4/2015 | 11:23:17 AM |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime  
"2/3/2015"
```

```
SmBackupId      : 113  
SmJobId         : 2032  
StartDateTime   : 2/2/2015 6:57:03 AM  
EndDateTime     : 2/2/2015 6:57:11 AM  
Duration        : 00:00:07.3060000  
CreatedDateTime : 2/2/2015 6:57:23 AM  
Status          : Completed  
ProtectionGroupName : Clone  
SmProtectionGroupId : 34  
PolicyName      : Vault  
SmPolicyId      : 18  
BackupName      : Clone_SCSPR0019366001_02-02-2015_06.57.08  
VerificationStatus : NotVerified
```

```
SmBackupId      : 114  
SmJobId         : 2183  
StartDateTime   : 2/2/2015 1:02:41 PM  
EndDateTime     : 2/2/2015 1:02:38 PM  
Duration        : -00:00:03.2300000  
CreatedDateTime : 2/2/2015 1:02:53 PM  
Status          : Completed  
ProtectionGroupName : Clone  
SmProtectionGroupId : 34  
PolicyName      : Vault  
SmPolicyId      : 18  
BackupName      : Clone_SCSPR0019366001_02-02-2015_13.02.45  
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable        : False
IsRestartable        : False
IsCompleted          : False
IsVisible            : True
IsScheduled          : False
PercentageCompleted : 0
Description          :
Status              : Queued
Owner                :
Error                :
Priority             : None
Tasks                : {}
ParentJobID          : 0
EventId              : 0
JobTypeId            :
ApisJobKey           :
ObjectId             : 0
PluginCode           : NONE
PluginName           :
```

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"](#).

## Überwachen von MySQL-Wiederherstellungsvorgängen

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 von MySQL-Ressourcensicherungen

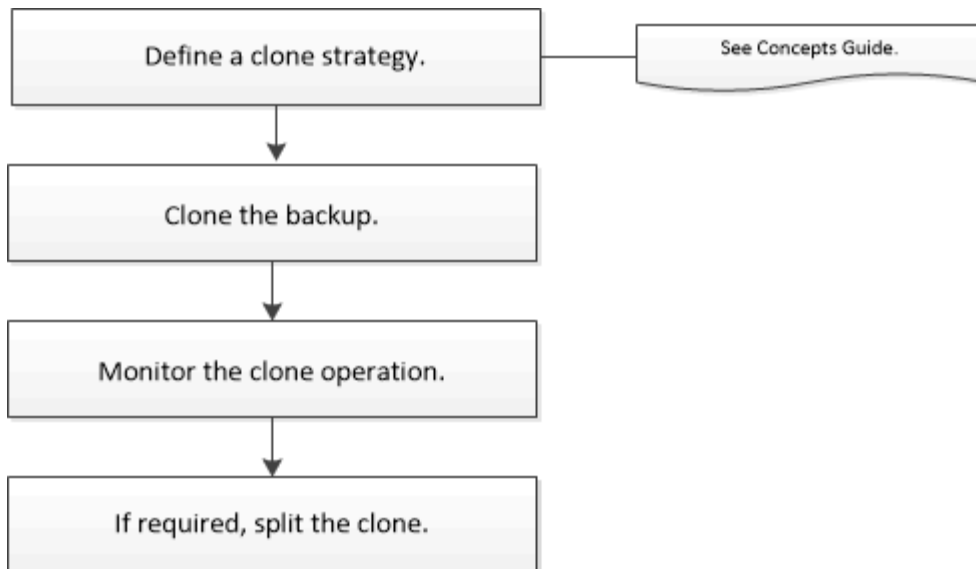
### Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

#### Informationen zu diesem Vorgang

- Sie können auf dem MySQL-Quellserver klonen.
- Sie können Ressourcensicherungen aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Für Datenextraktions- und Manipulationstools beim Befüllen von Data Warehouses
  - So stellen Sie versehentlich gelöschte oder geänderte Daten wieder her

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten detaillierte Informationen zu PowerShell-Cmdlets.

## Klonen Sie ein MySQL-Backup

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen.

### Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Bei Befehlen vor oder nach dem Klonen sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: `C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
  - Standardspeicherort auf dem Linux-Host: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl. \* Für die MySQL-Version 5.7 sollten Sie in der MySQL-Eigenschaftendatei `IGNORE_MYSQLX_PORT = true` (standardmäßig `false`) festlegen.

### Informationen zu diesem Vorgang

- Sie können die geklonten MySQL-Instanzen nicht schützen.
- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume"] .
- Bei ONTAP 9.12.1 und früheren 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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:

| Für dieses Feld...    | Machen Sie Folgendes...                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------|
| Server klonen         | Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.                              |
| Hafen                 | Geben Sie den Port an, auf dem die geklonte MySQL-Instanz gestartet werden soll.               |
| NFS-Export-IP-Adresse | Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden. |

7. Führen Sie auf der Seite „Skripts“ die folgenden Schritte aus:



Die Skripte werden auf dem Plug-in-Host ausgeführt.

- a. Geben Sie die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
  - Befehl vor dem Klonen: Löschen Sie vorhandene Datenbanken mit demselben Namen
  - Befehl nach dem Klonen: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.
- b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Mount-Befehl für ein Volume oder einen Qtree auf einer Linux-Maschine:

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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.

- Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
- Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

## PowerShell-Cmdlets

### Schritte

- Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer.

```
PS C:\> Open-SmConnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

- Rufen Sie die Sicherungen ab, um den Klonvorgang mithilfe des Cmdlets „`Get-SmBackup`“ durchzuführen.

Dieses Beispiel zeigt, dass zwei Sicherungen zum Klonen verfügbar sind:

```
C:\PS> Get-SmBackup
```

| BackupId             | BackupName                    |
|----------------------|-------------------------------|
| BackupTime           | BackupType                    |
| -----                | -----                         |
| 1                    | Payroll Dataset_vise-f6_08... |
| 8/4/2015 11:02:32 AM | Full Backup                   |
| 2                    | Payroll Dataset_vise-f6_08... |
| 8/4/2015 11:23:17 AM |                               |

- Starten Sie einen Klonvorgang von einer vorhandenen Sicherung und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

Dieses Beispiel zeigt, dass das zu klonende Backup eine NFSExportIPs-Adresse von 10.32.212.14 hat:

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName  
"scs000211748_gdl_englab_netapp_com_MySQL_mysqlid_3306_scs000211748_0  
6-26-2024_06.08.35.4307" -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqlid_3306"}  
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```



Wenn NFSExportIPs nicht angegeben ist, wird der Standardwert auf den Klonzielhost exportiert.

4. Überprüfen Sie, ob die Sicherungen erfolgreich geklont wurden, indem Sie mit dem Cmdlet „Get-SmCloneReport“ die Details des Klonauftrags anzeigen.

Sie können Details wie Klon-ID, Startdatum und -uhrzeit sowie Enddatum und -uhrzeit anzeigen.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration              : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName            : OnDemand_Clone
SmPolicyId            : 4
BackupPolicyName      : OnDemand_Full_Log
SmBackupPolicyId      : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName             : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

## Überwachen von MySQL-Klonvorgängen

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**.

## 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 <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme         | Wählen Sie <b>Pfad</b> 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"](#)

## Löschen oder Aufteilen von MySQL-Datenbankklonen nach dem Upgrade von SnapCenter

Nach dem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource aufteilen, aus der die Klone erstellt wurden.

### Informationen zu diesem Vorgang

Wenn Sie den Speicherbedarf der versteckten Klone ermitteln möchten, führen Sie den folgenden Befehl aus:  
`Get-SmClone -ListStorageFootprint`

### Schritte

1. Löschen Sie die Sicherungen der geklonten Ressourcen mithilfe des Cmdlets „remove-smbbackup“.
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mithilfe des Cmdlets „remove-smresourcegroup“.
3. Entfernen Sie den Schutz der geklonten Ressource mithilfe des Cmdlets „remove-smprotectresource“.
4. Wählen Sie die übergeordnete Ressource auf der Seite „Ressourcen“ aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht „Kopien verwalten“ die Klone entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
6. Wählen Sie die Klone aus und klicken Sie dann auf  , um Klone zu löschen, oder klicken Sie auf  um die Klone zu teilen.
7. Klicken Sie auf **OK**.



# Schützen Sie Anwendungen mit von NetApp unterstützten Plug-ins

## Von NetApp unterstützte Plug-Ins

### Übersicht der von NetApp unterstützten Plug-ins

Sie können die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und das Storage-Plug-in für die von Ihnen genutzten Anwendungen verwenden und diese Anwendungen dann mit SnapCenter sichern, wiederherstellen oder klonen. Ihre von NetApp unterstützten Plug-ins fungieren als hostseitige Komponenten der NetApp SnapCenter -Software und ermöglichen anwendungsbewussten Datenschutz und die Verwaltung von Ressourcen.

Wenn von NetApp unterstützte Plug-Ins installiert sind, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und die NetApp SnapVault -Technologie verwenden, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen. Die von NetApp unterstützten Plug-Ins können sowohl in Windows- als auch in Linux-Umgebungen verwendet werden.



SnapCenterCLI unterstützt keine von NetApp unterstützten Plug-In-Befehle.

NetApp stellt das Storage-Plug-in bereit, um Datenschutzvorgänge des Datenvolumens auf dem ONTAP Speicher mithilfe des in SnapCenter integrierten Plug-in-Frameworks durchzuführen.

Sie können die von NetApp unterstützten Plug-Ins von der Seite „Host hinzufügen“ aus installieren.

["Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts."](#)



Die Supportrichtlinien von SnapCenter decken den Support für das Plug-in-Framework, die Core Engine und die zugehörigen APIs ab. Der Support umfasst nicht den Plug-in-Quellcode und die zugehörigen Skripte, die auf dem Plug-in-Framework basieren.

### Was Sie mit den von NetApp unterstützten Plug-ins tun können

Sie können die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB und das Storage-Plug-in für Datenschutzvorgänge verwenden.

- Fügen Sie Ressourcen wie Datenbanken, Instanzen, Dokumente oder Tablespace hinzu.
- Erstellen Sie Backups.
- Aus Backups wiederherstellen.
- Klonen Sie Backups.
- Planen Sie Sicherungsvorgänge.
- Überwachen Sie Sicherungs-, Wiederherstellungs- und Klonvorgänge.
- Zeigen Sie Berichte zu Sicherungs-, Wiederherstellungs- und Klonvorgängen an.

Sie können die von NetApp unterstützten Plug-Ins für Datenschutzvorgänge verwenden.

- Erstellen Sie Snapshots der Konsistenzgruppe der Speichervolumes über ONTAP -Cluster hinweg.
- Sichern Sie benutzerdefinierte Anwendungen mithilfe des integrierten Pre- und Post-Scripting-Frameworks

Sie können ein ONTAP Volume, LUN oder einen Qtree sichern.

- Aktualisieren Sie Snapshots, die auf dem primären Server erstellt wurden, auf einen ONTAP Sekundärserver und nutzen Sie dabei die vorhandene Replikationsbeziehung (SnapVault/SnapMirror/vereinheitlichte Replikation) mithilfe der SnapCenter Richtlinie

ONTAP Primär- und Sekundärserver können ONTAP FAS, AFF, ASA, ONTAP Select oder Cloud Volumes ONTAP sein.

- Stellen Sie das komplette ONTAP Volume, LUN oder Dateien wieder her.

Sie sollten den jeweiligen Dateipfad manuell angeben, da die Such- oder Indizierungsfunktionen nicht in das Produkt integriert sind.

Qtree- oder Verzeichniswiederherstellung wird nicht unterstützt, Sie können jedoch nur den Qtree klonen und exportieren, wenn der Sicherungsumfang auf Qtree-Ebene definiert ist.

## Von NetApp unterstützte Plug-In-Funktionen

SnapCenter lässt sich in die Plug-in-Anwendung und in NetApp -Technologien auf dem Speichersystem integrieren. Um mit von NetApp unterstützten Plug-Ins wie MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und Storage-Plug-in zu arbeiten, verwenden Sie die grafische Benutzeroberfläche von SnapCenter .

- **Einheitliche grafische Benutzeroberfläche**

Die SnapCenter Schnittstelle bietet Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs-, Wiederherstellungs- und Klonvorgänge über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen.

- **Automatisierte zentrale Verwaltung**

Sie können Sicherungsvorgänge planen, die richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge durchführen. Sie können Ihre Umgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Technologie**

SnapCenter verwendet die NetApp Snapshot-Technologie mit den von NetApp unterstützten Plug-Ins zum Sichern von Ressourcen. Snapshots verbrauchen nur minimalen Speicherplatz.

Die von NetApp unterstützten Plug-Ins bieten außerdem die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung

Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktbezogener Kopien von Ressourcen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

Auf dem Speichersystem, auf dem Sie den Klon erstellen möchten, ist eine FlexClone -Lizenz erforderlich.

- Unterstützung für die Consistency Group (CG) Snapshot-Funktion von ONTAP als Teil der Backup-Erstellung.
- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Ressourcenhosts auszuführen

In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mithilfe externer Befehle.
- Möglichkeit zum Erstellen dateisystemkonsistenter Snapshots in Windows-Umgebungen.

## Von NetApp unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen auf physischen und virtuellen Maschinen. Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie von NetApp unterstützte Plug-Ins installieren.

| Maschine                                                                                       | Speichertyp                                                                                                                       |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Physische und NFS-Direktmounts auf den VM-Hosts (VMDKs und RDM-LUNs werden nicht unterstützt.) | FC-verbundene LUNs                                                                                                                |
| Physische und NFS-Direktmounts auf den VM-Hosts (VMDKs und RDM-LUNs werden nicht unterstützt.) | Über iSCSI verbundene LUNs                                                                                                        |
| Physische und NFS-Direktmounts auf den VM-Hosts (VMDKs und RDM-LUNs werden nicht unterstützt.) | Über NFS verbundene Volumes                                                                                                       |
| VMware ESXi                                                                                    | vVol-Datenspeicher auf NFS und SAN<br><br>vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden. |

## Für das von NetApp unterstützte Plug-In sind mindestens ONTAP -Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen

- Jobstopp
- LUN-Attribut anzeigen
- LUN erstellen
- LUN löschen
- LUN-Geometrie
- lun igroup hinzufügen
- lun igroup erstellen
- LUN-Igroup löschen
- LUN-Igroup umbenennen
- lun igroup show
- LUN-Zuordnung Add-Reporting-Nodes
- LUN-Zuordnung erstellen
- LUN-Zuordnung löschen
- LUN-Zuordnung zum Entfernen von Berichtsknoten
- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Netzwerkschnittstelle
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start

- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen
- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen
- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle

## Bereiten Sie Speichersysteme für die SnapMirror und SnapVault -Replikation für von NetApp unterstützte Plug-Ins vor

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs durchgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.



Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.



SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im ["ONTAP-Dokumentation"](#).

## Definieren Sie eine Sicherungsstrategie

Durch das Definieren einer Sicherungsstrategie vor dem Erstellen Ihrer Sicherungsaufträge wird sichergestellt, dass Sie über die Sicherungen verfügen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Ressourcen benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

### Informationen zu diesem Vorgang

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

### Schritte

1. Bestimmen Sie, wann Sie Ihre Ressourcen sichern sollten.
2. Entscheiden Sie, wie viele Sicherungsaufträge Sie benötigen.
3. Entscheiden Sie, wie Sie Ihre Backups benennen möchten.

4. Entscheiden Sie, ob Sie Konsistenzgruppen-Snapshots möchten, und entscheiden Sie sich für geeignete Optionen zum Löschen von Konsistenzgruppen-Snapshots.
5. Entscheiden Sie, ob Sie die NetApp SnapMirror -Technologie für die Replikation oder die NetApp SnapVault -Technologie für die langfristige Aufbewahrung verwenden möchten.
6. Bestimmen Sie die Aufbewahrungsdauer für die Snapshots auf dem Quellspeichersystem und dem SnapMirror -Ziel.
7. Legen Sie fest, ob Sie vor oder nach dem Sicherungsvorgang Befehle ausführen möchten, und geben Sie ein Präskript oder Postskript an.

## Sicherungsstrategie für von NetApp unterstützte Plug-Ins

### Sicherungspläne für von NetApp unterstützte Plug-In-Ressourcen

Der wichtigste Faktor bei der Festlegung eines Sicherungszeitplans ist die Änderungsrate der Ressource. Je häufiger Sie Ihre Ressourcen sichern, desto weniger Archivprotokolle muss SnapCenter für die Wiederherstellung verwenden, was zu schnelleren Wiederherstellungsvorgängen führen kann.

Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service-Level-Agreement (SLA) und Ihr Recovery Point Objective (RPO).

SLA definiert das erwartete Serviceniveau und befasst sich mit vielen servicebezogenen Problemen, einschließlich der Verfügbarkeit und Leistung des Dienstes. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins auch Zeitplantyp genannt, ist Teil einer Richtlinienkonfiguration. Sie können die Sicherungshäufigkeit beispielsweise auf stündlich, täglich, wöchentlich oder monatlich konfigurieren. Sie können in der SnapCenter -GUI auf Richtlinien zugreifen, indem Sie auf **Einstellungen > Richtlinien** klicken.

- Sicherungszeitpläne

Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können in der SnapCenter -GUI auf die Zeitpläne der Ressourcengruppe zugreifen, indem Sie auf **Ressourcen** klicken, dann das entsprechende Plug-In auswählen und auf **Anzeigen > Ressourcengruppe** klicken.

### Anzahl der benötigten Sicherungsaufträge

Zu den Faktoren, die die Anzahl der benötigten Sicherungsaufträge bestimmen, gehören die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Die Anzahl der von Ihnen ausgewählten Sicherungsaufträge hängt normalerweise von der Anzahl der Datenträger ab, auf denen Sie Ihre Ressourcen platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Ressourcen auf einem Volume und eine große Ressource auf einem anderen Volume platziert haben, können Sie einen Sicherungsauftrag für die kleinen Ressourcen und einen Sicherungsauftrag für die große Ressource erstellen.

## **Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte, von NetApp unterstützte Plug-in-Ressourcen unterstützt werden**

Sie müssen eine Strategie definieren, bevor Sie Wiederherstellungsvorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte, von NetApp unterstützte Plug-In-Ressourcen.



Sie können manuell hinzugefügte, von NetApp unterstützte Plug-In-Ressourcen nicht wiederherstellen.

### **Vollständige Ressourcenwiederherstellung**

- Stellt alle Volumes, Qtrees und LUNs einer Ressource wieder her



Wenn die Ressource Volumes oder Qtrees enthält, werden die Snapshots, die nach dem zur Wiederherstellung ausgewählten Snapshot auf diesen Volumes oder Qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn außerdem eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

### **Wiederherstellung auf Dateiebene**

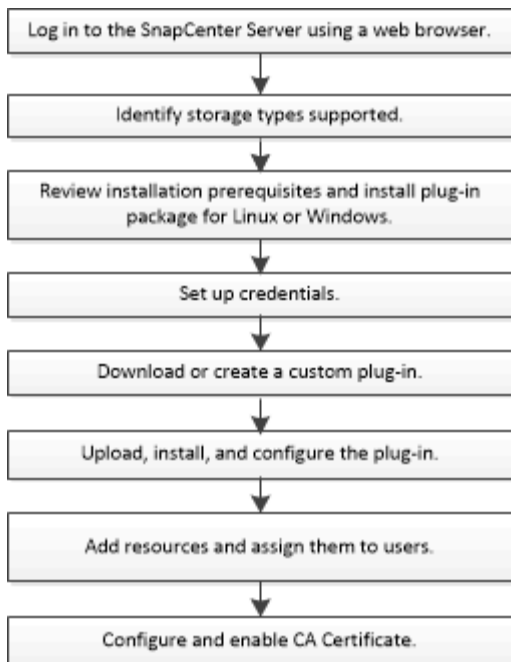
- Stellt Dateien aus Volumes, Qtrees oder Verzeichnissen wieder her
- Stellt nur die ausgewählten LUNs wieder her

## **Bereiten Sie die Installation von NetApp unterstützten Plug-Ins vor**

### **Installationsablauf der von SnapCenter NetApp unterstützten Plug-Ins**

Sie sollten von SnapCenter NetApp unterstützte Plug-Ins installieren und einrichten, wenn Sie von NetApp unterstützte Plug-In-Ressourcen schützen möchten.





## Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-In-Paketen für Windows, Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-In-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Die von NetApp unterstützten Plug-Ins werden in Windows-, Linux- und AIX-Umgebungen unterstützt.



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

- Sie müssen Java 11 auf Ihrem Linux-, Windows- oder AIX-Host installiert haben.



IBM Java wird auf Windows- und Linux-Hosts nicht unterstützt.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB und Storage-Plug-in müssen auf dem Client-Host verfügbar sein, von dem aus der Vorgang zum Hinzufügen des Hosts ausgeführt wird.

### Allgemein

Wenn Sie iSCSI verwenden, sollte der iSCSI-Dienst ausgeführt werden.

### Windows-Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten und lokalen Anmeldeberechtigungen auf dem Remotehost verfügen.
- Wenn Sie Clusterknoten in SnapCenter verwalten, benötigen Sie einen Benutzer mit Administratorrechten für alle Knoten im Cluster.

- Sie müssen das SnapCenter Plug-in für Microsoft Windows manuell auswählen.

["JAVA für Windows herunterladen"](#)

## Linux- und AIX-Hosts



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

- Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder Nicht-Root-Benutzer aktiviert haben.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

Wenn Sie Windows Server 2019 oder Windows Server 2016 für den SnapCenter Server-Host verwenden, müssen Sie Java 11 installieren. Das Interoperability Matrix Tool (IMT) enthält die neuesten Informationen zu den Anforderungen.

["Laden Sie JAVA für Linux herunter"](#)

["Laden Sie JAVA für AIX herunter"](#)

["NetApp Interoperabilitätsmatrix-Tool"](#)

- Sie müssen Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu gewähren. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.



Stellen Sie sicher, dass Sie Sudo Version 1.8.7 oder höher verwenden.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

*LINUX\_USER* ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den *Prüfsummenwert* aus der Datei **sc\_unix\_plugins\_checksum.txt** abrufen, die sich hier befindet:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc\_unix\_plugins\_checksum.txt*, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc\_unix\_plugins\_checksum.txt*, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

**AIX-Hostanforderungen**

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

- 
- Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.
- 
- Das SnapCenter -Plug-in für UNIX, das Teil des SnapCenter Plug-in-Pakets für AIX ist, unterstützt keine gleichzeitigen Volume-Gruppen.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | AIX 7.1 oder höher                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 4 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <div>2 GB</div> <div> 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.</div> |

| Artikel                      | Anforderungen                                                                                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Erforderliche Softwarepakete | <p>Java 11 IBM Java</p> <p>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.</p> |

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#) .

### Konfigurieren Sie Sudo-Berechtigungen für Nicht-Root-Benutzer für den AIX-Host

SnapCenter 4.4 und höher ermöglicht es einem Nicht-Root-Benutzer, das SnapCenter Plug-ins-Paket für AIX zu installieren und den Plug-in-Prozess zu starten. Die Plug-In-Prozesse werden als effektiver Nicht-Root-Benutzer ausgeführt. Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen.

### Was Sie brauchen

- Sudo Version 1.8.7 oder höher.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um die Algorithmen für den Nachrichtenauthentifizierungscode zu konfigurieren: MACs hmac-sha2-256 und MACs hmac-sha2-512.

Starten Sie den SSHD-Dienst nach der Aktualisierung der Konfigurationsdatei neu.

Beispiel:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

### Über diese Aufgabe

Sie sollten Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um Zugriff auf die folgenden Pfade zu gewähren:

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/benutzerdefinierter_Speicherort/ NetApp/snapcenter/spl/installation/plugins/uninstall`

- /benutzerdefinierter\_Speicherort/ NetApp/snapcenter/spl/bin/spl

## Schritte

1. Melden Sie sich beim AIX-Host an, auf dem Sie das SnapCenter Plug-ins-Paket für AIX installieren möchten.
2. Fügen Sie mithilfe des Linux-Dienstprogramms visudo die folgenden Zeilen zur Datei /etc/sudoers hinzu.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



Wenn Sie ein RAC-Setup haben, sollten Sie neben den anderen zulässigen Befehlen Folgendes zur Datei /etc/sudoers hinzufügen: „/<crs\_home>/bin/olsnodes“

Sie können den Wert von *crs\_home* aus der Datei /etc/oracle/olr.loc abrufen.

*AIX\_USER* ist der Name des von Ihnen erstellten Nicht-Root-Benutzers.

Sie können den Prüfsummenwert aus der Datei **sc\_unix\_plugins\_checksum.txt** abrufen, die sich hier befindet:

- C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc\_unix\_plugins\_checksum.txt, wenn SnapCenter Server auf einem Windows-Host installiert ist.
- /opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc\_unix\_plugins\_checksum.txt, wenn SnapCenter Server auf einem Linux-Host installiert ist.



Das Beispiel sollte nur als Referenz für die Erstellung Ihrer eigenen Daten verwendet werden.

## Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems

vertraut sein.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | Microsoft Windows<br><br>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | 5 GB<br><br> 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.                                                                                                         |
| Erforderliche Softwarepakete                                                                 | <ul style="list-style-type: none"><li>• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket</li><li>• PowerShell Core 7.4.2</li><li>• Java 11 Oracle Java und OpenJDK</li></ul> <p>Java 11 Oracle Java und OpenJDK werden nur für SAP HANA, IBM Db2, PostgreSQL, MySQL, von NetApp unterstützte Plug-Ins und andere benutzerdefinierte Anwendungen benötigt, die auf einem Windows-Host installiert werden können.</p> <p>Die neuesten Informationen zu unterstützten Versionen finden Sie im <a href="#">"NetApp Interoperabilitätsmatrix-Tool"</a> .</p> |

## Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux und AIX

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



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

| Artikel                                                                                      | Anforderungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Betriebssysteme                                                                              | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• Oracle Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul>                                                                                                                                                                                                                                                                                                                                          |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 1 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | 2 GB <div>  <p>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.</p> </div> |
| Erforderliche Softwarepakete                                                                 | Java 11 Oracle Java oder OpenJDK <p>Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter <code>/var/opt/snapcenter/spl/etc/spl.properties</code> auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.</p>                                                                                                                                                                                                    |

Die neuesten Informationen zu unterstützten Versionen finden Sie im ["NetApp Interoperabilitätsmatrix-Tool"](#)

## Einrichten von Anmeldeinformationen für von NetApp unterstützte Plug-Ins

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Datenbanken oder Windows-Dateisystemen erstellen.

### Bevor Sie beginnen

- Linux- oder AIX-Hosts

Sie müssen Anmeldeinformationen für die Installation von Plug-Ins auf Linux- oder AIX-Hosts einrichten.

Sie müssen die Anmeldeinformationen für den Root-Benutzer oder für einen Nicht-Root-Benutzer mit Sudo-Berechtigungen einrichten, um den Plug-In-Prozess zu installieren und zu starten.

**Best Practice:** Obwohl Sie Anmeldeinformationen für Linux erstellen dürfen, nachdem Sie Hosts bereitgestellt und Plug-Ins installiert haben, besteht die Best Practice darin, Anmeldeinformationen nach dem Hinzufügen von SVMs zu erstellen, bevor Sie Hosts bereitstellen und Plug-Ins installieren.

- Windows-Hosts

Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.

Sie müssen die Anmeldeinformationen mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

- Von NetApp unterstützte Plug-In-Anwendungen

Das Plug-In verwendet die Anmeldeinformationen, die beim Hinzufügen einer Ressource ausgewählt oder erstellt werden. Wenn für eine Ressource während Datenschutzvorgängen keine Anmeldeinformationen erforderlich sind, können Sie die Anmeldeinformationen auf **Keine** festlegen.

### Informationen zu diesem Vorgang

Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite **Anmeldeinformationen** die zum Konfigurieren der Anmeldeinformationen erforderlichen Informationen an:

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |



| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzername                      | <p>Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen.</p> <ul style="list-style-type: none"> <li>• Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe</li> </ul> <p>Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind:</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\Benutzername</i></li> <li>◦ <i>Domänen-FQDN\Benutzername</i></li> <li>• Lokaler Administrator (nur für Arbeitsgruppen)</li> </ul> <p>Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ ist: <i>Benutzername</i></p> |
| Passwort                          | Geben Sie das zur Authentifizierung verwendete Passwort ein.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Authentifizierungstyp             | Wählen Sie den Authentifizierungstyp aus, den Sie verwenden möchten.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen <b>Sudo-Berechtigungen verwenden</b>, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p> <div>  <p>Gilt nur für Linux- und AIX-Benutzer.</p> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise die Anmeldeinformationsverwaltung einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ zuweisen.

## Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

### Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

### Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -Effectivelmmmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
  - a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
domainName\accountName$  
.. Fügen Sie der Gruppe Computerobjekte hinzu.  
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu erstellen.
```

Zum Beispiel,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des  
Dienstkontos.
```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:
  - a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

| Display Name                         | Name               | Install State |
|--------------------------------------|--------------------|---------------|
| -----                                | ----               | -----         |
| [ ] Active Directory Domain Services | AD-Domain-Services | Available     |

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

| Success | Restart Needed | Exit Code | Feature Result                                |
|---------|----------------|-----------|-----------------------------------------------|
| -----   | -----          | -----     | -----                                         |
| True    | No             | Success   | {Active Directory Domain Services, Active ... |

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- Starten Sie Ihren Host neu.
  - Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`
  - Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`
- Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
  - Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

## Installieren Sie die von NetApp unterstützten Plug-Ins

### Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und die Plug-in-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren.

#### Bevor Sie beginnen

- Sie sollten ein Benutzer sein, dem eine Rolle zugewiesen ist, die über die Berechtigungen zum Installieren und Deinstallieren von Plug-Ins verfügt, beispielsweise die SnapCenter Administratorrolle.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

"Konfigurieren Sie ein gruppenverwaltetes Dienstkonto auf Windows Server 2016 oder höher für benutzerdefinierte Anwendungen"

- Für den Windows-Host müssen Sie sicherstellen, dass Sie das SnapCenter -Plug-in für Windows auswählen.

## Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Wenn Sie Plug-Ins auf einem Cluster (WSFC) installieren, werden die Plug-Ins auf allen Knoten des Clusters installiert.

## Schritte

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

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosttyp            | <p>Wählen Sie den Hosttyp aus:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> <li>• AIX</li> </ul> <div>  <p>Die von NetApp unterstützten Plug-Ins können in Windows-, Linux- und AIX-Umgebungen verwendet werden.</p> </div> <div>  <p>Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.</p> </div> |

| Für dieses Feld...   | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hostname             | <p>Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.</p> <p>SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p> <p>In Windows-Umgebungen wird die IP-Adresse für nicht vertrauenswürdige Domänenhosts nur unterstützt, wenn sie in den FQDN aufgelöst wird.</p> <p>Sie können die IP-Adressen oder den FQDN eines eigenständigen Hosts eingeben.</p> <p>Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.</p>                                                                                                                          |
| Anmeldeinformationen | <p>Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen.</p> <p>Die Anmeldeinformationen müssen über Administratorrechte auf dem Remotehost verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen von Anmeldeinformationen.</p> <p>Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen.</p> <div>  <p>Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.</p> </div> |

5. Wählen Sie im Abschnitt **Zu installierende Plug-ins auswählen** die zu installierenden Plug-ins aus.

Sie können die folgenden Plug-Ins aus der Liste installieren:

- MongoDB
- ORASCPM (angezeigt als Oracle-Anwendungen)
- SAP ASE
- SAP MaxDB
- Storage

6. (Optional) Wählen Sie **Weitere Optionen**, um die anderen Plug-Ins zu installieren.

| Für dieses Feld...                     | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hafen                                  | <p>Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an.</p> <p>Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.</p> <div data-bbox="873 512 927 569">  </div> <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> |
| Installationspfad                      | <p>Die von NetApp unterstützten Plug-Ins können entweder auf einem Windows- oder einem Linux-System installiert werden.</p> <ul style="list-style-type: none"> <li>Für das SnapCenter Plug-ins-Paket für Windows ist der Standardpfad C:\Programme\NetApp\ SnapCenter.</li> </ul> <p>Optional können Sie den Pfad anpassen.</p> <ul style="list-style-type: none"> <li>Für SnapCenter Plug-ins Package für Linux und SnapCenter Plug-ins Package für AIX ist der Standardpfad /opt/NetApp/snapcenter .</li> </ul> <p>Optional können Sie den Pfad anpassen.</p>                  |
| Vorinstallationsprüfungen überspringen | <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                    |

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen | <p>Aktivieren Sie für Windows-Hosts dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten.</p> <div>  <p>Geben Sie den gMSA-Namen im folgenden Format an:<br/>Domänenname\Kontoname\$.</p> </div> <div>  <p>gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.</p> </div> |

## 7. Wählen Sie **Senden**.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird überprüft, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt.

Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei web.config aktualisieren, die sich unter `C:\Program Files\NetApp\SnapCenter WebApp`, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.



Wenn Sie in einem HA-Setup SnapManager.Web.UI.dll.config aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren und den SnapCenter App Pool neu starten.

Der Windows-Standardpfad ist `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

Der Standardpfad für Linux ist

`/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

## 8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und wählen Sie dann **Bestätigen und senden**.



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/Protokolle`.

## Installieren Sie SnapCenter Plug-in-Pakete für Linux, Windows oder AIX auf mehreren Remote-Hosts mithilfe von Cmdlets

Sie können die SnapCenter -Plug-in-Pakete für Linux, Windows oder AIX mithilfe des PowerShell-Cmdlets „Install-SmHostPackage“ gleichzeitig auf mehreren Hosts installieren.

### Bevor Sie beginnen

Der Benutzer, der einen Host hinzufügt, sollte über Administratorrechte für den Host verfügen.



Speicher- und Oracle-Anwendungen werden unter AIX unterstützt.

### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host mit dem Cmdlet „Open-SmConnection“ eine Sitzung ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-In auf mehreren Hosts mithilfe des Cmdlets Install-SmHostPackage und der erforderlichen Parameter.

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"](#) .

Sie können die Option -skippercheck verwenden, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

## Installieren Sie die von NetApp unterstützten Plug-Ins auf Linux-Hosts mithilfe der Befehlszeilenschnittstelle

Sie sollten die von NetApp unterstützten Plug-Ins mithilfe der SnapCenter -Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung keine Remote-Installation des Plug-Ins über die SnapCenter Benutzeroberfläche zulässt, können Sie die von NetApp unterstützten Plug-Ins entweder im Konsolenmodus oder im Hintergrundmodus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

### Schritte

1. Kopieren Sie die Installationsdatei des SnapCenter Plug-ins-Pakets für Linux (snapcenter\_linux\_host\_plugin.bin) von C:\ProgramData\NetApp\ SnapCenter\Package Repository auf den Host, auf dem Sie die von NetApp unterstützten Plug-ins installieren möchten.

Sie können auf diesen Pfad von dem Host aus zugreifen, auf dem der SnapCenter -Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei kopiert haben.
3. Installieren Sie das Plug-In:

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```



- -DPORT gibt den SMCore HTTPS-Kommunikationsport an.
- -DSERVER\_IP gibt die IP-Adresse des SnapCenter -Servers an.
- -DSERVER\_HTTPS\_PORT gibt den HTTPS-Port des SnapCenter -Servers an.
- -DUSER\_INSTALL\_DIR gibt das Verzeichnis an, in dem Sie das SnapCenter Plug-Ins-Paket für Linux installieren möchten.
- \_DINSTALL\_LOG\_NAME gibt den Namen der Protokolldatei an.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Fügen Sie den Host mit dem Cmdlet Add-Smhost und den erforderlichen Parametern zum SnapCenter -Server hinzu.

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 ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

5. Melden Sie sich bei SnapCenter an und laden Sie das von NetApp unterstützte Plug-In über die Benutzeroberfläche oder mithilfe von PowerShell-Cmdlets hoch.

Sie können das von NetApp unterstützte Plug-In von der Benutzeroberfläche hochladen, indem Sie auf ["Hosts hinzufügen und Plug-in-Pakete auf Remote-Hosts installieren"](#) Abschnitt.

Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets.

["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Überwachen Sie den Status der Installation von NetApp unterstützten Plug-Ins

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**.

## CA-Zertifikat konfigurieren

### CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.



Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter ["So generieren Sie eine CA-Zertifikat-CSR-Datei"](#).



Wenn Sie das CA-Zertifikat für Ihre Domäne (\*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (\*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

### CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

## Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsolle (MMC) und klicken Sie dann auf **Datei > Snap-In hinzufügen/entfernen**.

2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm > Zertifikate – Lokaler Computer > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben > Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

| In diesem Assistentenfenster ...             | Gehen Sie wie folgt vor...                                                                                                         |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Privaten Schlüssel importieren               | Wählen Sie die Option <b>Ja</b> , importieren Sie den privaten Schlüssel und klicken Sie anschließend auf <b>Weiter</b> .          |
| Importdateiformat                            | Nehmen Sie keine Änderungen vor; klicken Sie auf <b>Weiter</b> .                                                                   |
| Sicherheit                                   | Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf <b>Weiter</b> . |
| Abschließen des Zertifikatimport-Assistenten | Überprüfen Sie die Zusammenfassung und klicken Sie dann auf <b>Fertig</b> , um den Import zu starten.                              |



Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: \*.pfx, \*.p12 und \*.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

### Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

#### Schritte

1. Führen Sie auf der GUI Folgendes aus:
  - a. Doppelklicken Sie auf das Zertifikat.
  - b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
  - c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
  - d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
  - e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:

- a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

```
Get-ChildItem -Pfad Zertifikat:\LocalMachine\My
```

- b. Kopieren Sie den Fingerabdruck.

### Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

#### Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Beispiel:

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-In-Dienste, indem Sie die folgenden Befehle ausführen:
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Beispiel:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

### Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten Plug-In-Dienst auf dem Linux-Host

Sie sollten das Kennwort des Plug-In-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den Plug-

In-Truststore konfigurieren und ein von der CA signiertes Schlüsselpaar für den Plug-In-Truststore mit dem SnapCenter -Plug-In-Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Die Plug-Ins verwenden die Datei „keystore.jks“, die sich unter `/opt/NetApp/snapcenter/scc/etc` befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Dies ist der Wert, der dem Schlüssel „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_in_cert" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE\_PASS in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher enthält: `/opt/NetApp/snapcenter/scc/etc`.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder
Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

#### Schritte

1. Navigieren Sie zu dem Ordner, der den Plug-In-Schlüsselspeicher /opt/ NetApp/snapcenter/scc/etc enthält.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkennwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE\_PASS in der Datei agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei
agent.properties.
```

Aktualisieren Sie diesen Wert anhand des Schlüssels `SCC_CERTIFICATE_ALIAS`.

8. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

### Konfigurieren der Zertifikatsperrliste (CRL) für Plug-Ins

#### Informationen zu diesem Vorgang

- SnapCenter Plug-ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist „opt/NetApp/snapcenter/scc/etc/crl“.

#### Schritte

1. Sie können das Standardverzeichnis in der Datei `agent.properties` anhand des Schlüssels `CRL_PATH` ändern und aktualisieren.

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

### Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten Plug-In-Dienst auf dem Windows-Host

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

Die Plug-ins verwenden die Datei `keystore.jks`, die sich unter `C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc` befindet, sowohl als Truststore als auch als Keystore.

**Verwalten Sie das Kennwort für den Plug-In-Schlüsselspeicher und den Alias des verwendeten, von der Zertifizierungsstelle signierten Schlüsselpaars.**

#### Schritte

1. Sie können das Standardkennwort für den Plug-in-Keystore aus der Eigenschaftendatei des Plug-in-Agenten abrufen.

Es handelt sich um den Wert, der dem Schlüssel `KEYSTORE_PASS` entspricht.

2. Ändern Sie das Keystore-Passwort:

```
keytool -storepasswd -keystore keystore.jks
```



Wenn der Befehl „keytool“ in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl „keytool“ durch seinen vollständigen Pfad.

```
C:\Programme\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

```
keytool -keypasswd -alias "Aliasname_im_Zertifikat" -keystore keystore.jks
```

Aktualisieren Sie dasselbe für den Schlüssel KEYSTORE\_PASS in der Datei *agent.properties*.

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



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

### Konfigurieren Sie Stamm- oder Zwischenzertifikate für den Plug-In-Truststore

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

#### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder Zwischenzertifikate für den Plug-In-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 Plug-In-Truststore

Sie sollten das von der Zertifizierungsstelle signierte Schlüsselpaar für den Truststore des Plug-Ins konfigurieren.

#### Schritte

1. Navigieren Sie zu dem Ordner mit dem Plug-in-Schlüsselspeicher *C:\Programme\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
keytool -list -v -keystore keystore.jks
```



4. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel hinzu.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.

```
keytool -list -v -keystore keystore.jks
```

6. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-Zertifikat in das Schlüsselspeicherkenwort.

Das Standardkennwort für den Plug-in-Schlüsselspeicher ist der Wert des Schlüssels KEYSTORE\_PASS in der Datei *agent.properties*.

```
keytool -keypasswd -alias "Aliasname_im_CA_Zertifikat" -keystore keystore.jks
```

8. Konfigurieren Sie den Aliasnamen aus dem CA-Zertifikat in der Datei *agent.properties*.

Aktualisieren Sie diesen Wert anhand des Schlüssels SCC\_CERTIFICATE\_ALIAS.

9. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den Plug-In-Truststore konfiguriert haben.

#### Konfigurieren der Zertifikatsperrliste (CRL) für SnapCenter -Plug-Ins

##### Informationen zu diesem Vorgang

- Um die neueste CRL-Datei für das entsprechende CA-Zertifikat herunterzuladen, siehe ["So aktualisieren Sie die Zertifikatsperrlistendatei im SnapCenter CA-Zertifikat"](#).
- SnapCenter Plug-Ins suchen in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SnapCenter -Plug-ins ist 'C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'.

##### Schritte

1. Sie können das Standardverzeichnis in der Datei *agent.properties* anhand des Schlüssels 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.

## Bereiten Sie sich auf den Datenschutz vor

### Voraussetzungen für die Verwendung der von NetApp unterstützten Plug-Ins

Bevor Sie die von SnapCenter NetApp unterstützten Plug-Ins verwenden, muss der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installieren und konfigurieren Sie SnapCenter Server.
- Melden Sie sich beim SnapCenter -Server an.
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen und gegebenenfalls Anmeldeinformationen erstellen.
- Fügen Sie Hosts hinzu und installieren und laden Sie die Plug-Ins hoch.
- Installieren Sie gegebenenfalls Java 11 auf dem Plug-In-Host.
- Wenn Sie über mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration verfügen, können Sie mithilfe der SnapCenter -CLI auf dem Datenbankhost Folgendes ausführen:
  - Standardmäßig werden alle IP-Adressen des Datenbankhosts zur NFS-Speicherexportrichtlinie in der Storage Virtual Machine (SVM) für die geklonten Volumes hinzugefügt. Wenn Sie eine bestimmte IP-Adresse haben oder auf eine Teilmenge der IP-Adressen beschränken möchten, führen Sie die CLI „Set-PreferredHostIPsInStorageExportPolicy“ aus.
  - Wenn Sie mehrere Datenpfade (LIFs) in SVMs haben, wählt SnapCenter den entsprechenden Datenpfad (LIF) zum Mounten des geklonten NFS-Volumes aus. Wenn Sie jedoch einen bestimmten

Datenpfad (LIF) angeben möchten, müssen Sie die CLI „Set-SvmPreferredDataPath“ ausführen. 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](#)".

- Richten Sie SnapMirror und SnapVault ein, wenn Sie eine Backup-Replikation wünschen.
- Stellen Sie sicher, dass Port 9090 von keiner anderen Anwendung auf dem Host verwendet wird.

Port 9090 muss zusätzlich zu den anderen von SnapCenter benötigten Ports für die Verwendung durch von NetApp unterstützte Plug-Ins reserviert werden.

## So werden Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von NetApp unterstützten Plug-In-Ressourcen verwendet

Bevor Sie SnapCenter verwenden, ist es hilfreich, die grundlegenden Konzepte im Zusammenhang mit den Sicherungs-, Klon- und Wiederherstellungsvorgängen zu verstehen, die Sie durchführen möchten. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind normalerweise Datenbanken, Windows-Dateisysteme oder VMs, die Sie mit SnapCenter sichern oder klonen.
- Eine SnapCenter -Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster.

Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem Zeitplan aus, den Sie für die Ressourcengruppe angeben.

Sie können bei Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Sicherungen für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Sicherungshäufigkeit, die Aufbewahrung von Kopien, Replikation, Skripte und andere Merkmale von Datenschutzvorgängen fest.

Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie eine bedarfsgesteuerte Sicherung für eine einzelne Ressource durchführen.

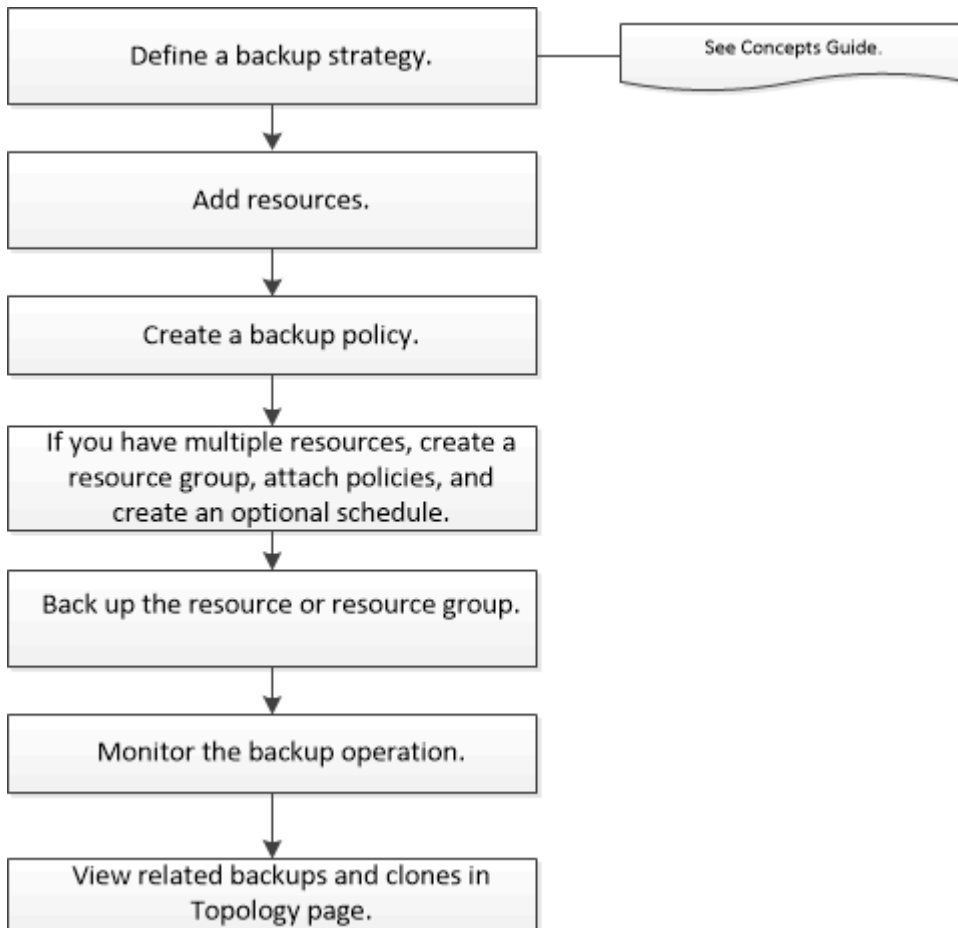
Stellen Sie sich eine Ressourcengruppe so vor, als würde sie definieren, *was* Sie schützen möchten und wann Sie es hinsichtlich Tag und Uhrzeit schützen möchten. Stellen Sie sich eine Richtlinie so vor, als würde sie definieren, *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme auf dem Host enthält. Sie könnten dann zwei Richtlinien an die Ressourcengruppe anhängen: eine tägliche Richtlinie und eine stündliche Richtlinie. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass täglich eine dateibasierte Sicherung durchgeführt wird, und einen anderen Zeitplan, der stündlich eine Snapshot-basierte Sicherung durchführt.

## Sichern Sie von NetApp unterstützte Plug-In-Ressourcen

## Sichern Sie von NetApp unterstützte Plug-In-Ressourcen

Der Sicherungsworkflow umfasst die Planung, die Identifizierung der Ressourcen für die Sicherung, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#)

## Ressourcen zu NetApp unterstützten Plug-ins hinzufügen

Sie müssen die Ressourcen hinzufügen, die Sie sichern oder klonen möchten. Abhängig von Ihrer Umgebung können die Ressourcen entweder Datenbankinstanzen oder Sammlungen sein, die Sie sichern oder klonen möchten.

### Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Sie müssen die Plug-Ins auf den SnapCenter -Server hochgeladen haben.

## Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ die Option „Ressource hinzufügen“ aus.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

| Für dieses Feld...      | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                    | Geben Sie den Namen der Ressource ein.                                                                                                                                                                                                                                                                                                                                                           |
| Hostname                | Wählen Sie den Host aus.                                                                                                                                                                                                                                                                                                                                                                         |
| Typ                     | <p>Wählen Sie den Typ aus. Der Typ wird gemäß der Plug-In-Beschreibungsdatei vom Benutzer definiert. Zum Beispiel Datenbank und Instanz.</p> <p>Falls der ausgewählte Typ ein übergeordnetes Element hat, geben Sie die Details des übergeordneten Elements ein. Wenn der Typ beispielsweise „Datenbank“ und das übergeordnete Element „Instanz“ ist, geben Sie die Details der Instanz ein.</p> |
| Anmeldeinformationsname | Wählen Sie Anmeldeinformationen aus oder erstellen Sie neue Anmeldeinformationen.                                                                                                                                                                                                                                                                                                                |
| Bergpfade               | Geben Sie die Mount-Pfade ein, in denen die Ressource gemountet ist. Dies gilt nur für einen Windows-Host.                                                                                                                                                                                                                                                                                       |

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ ein Speichersystem und ein oder mehrere Volumes, LUNs und Qtrees aus und wählen Sie dann **Speichern**.

Optional: Wählen Sie die  Symbol, um weitere Volumes, LUNs und Qtrees aus anderen Speichersystemen hinzuzufügen.



Von NetApp unterstützte Plug-Ins unterstützen keine automatische Erkennung der Ressourcen. Auch die Speicherdetails physischer und virtueller Umgebungen werden nicht automatisch erkannt. Sie müssen beim Erstellen der Ressourcen die Speicherinformationen für physische und virtuelle Umgebungen angeben.

5. Geben Sie auf der Seite „Ressourceneinstellungen“ benutzerdefinierte Schlüssel-Wert-Paare für die Ressource an.



Stellen Sie sicher, dass der Name des benutzerdefinierten Schlüssels in Großbuchstaben geschrieben ist.

#### Resource settings

| Name         | Value     |
|--------------|-----------|
| HOST         | localhost |
| PORT         | 3306      |
| MASTER_SLAVE | NO        |

Die jeweiligen Plug-In-Parameter finden Sie unter "[Parameter zum Konfigurieren der Ressource](#)"

6. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

### Ergebnis

Die Ressourcen werden zusammen mit Informationen wie Typ, Host- oder Clusternamen, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.



Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

### Nach Abschluss

Wenn Sie anderen Benutzern Zugriff auf die Assets gewähren möchten, muss der SnapCenter Administrator diesen Benutzern Assets zuweisen. Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

Nachdem Sie die Ressourcen hinzugefügt haben, können Sie die Ressourcendetails ändern. Wenn einer von NetApp unterstützten Plug-In-Ressourcen Sicherungen zugeordnet sind, können die folgenden Felder nicht geändert werden: Ressourcenname, Ressourcentyp und Hostname.

## Parameter zum Konfigurieren der Ressource

Wenn Sie die Plug-Ins manuell hinzufügen, können Sie die Ressource auf der Seite „Ressourceneinstellungen“ mit den folgenden Parametern konfigurieren.

### Plug-in für MongoDB

Ressourceneinstellungen:

- MONGODB\_APP\_SERVER=(für Ressourcentyp als Sharded Cluster) oder MONGODB\_REPLICASET\_SERVER=(für Ressourcentyp als Replikatsatz)
- OPLOG\_PATH=(Optionaler Parameter, falls er von MongoDB.propertiesfile bereitgestellt wird)
- MONGODB\_AUTHENTICATION\_TYPE= (PLAIN für LDAP-Authentifizierung und Keine für andere)

Sie müssen die folgenden Parameter in der Datei MongoDB.properties angeben:

- DISABLE\_STARTING\_STOPPING\_SERVICES=
  - N, wenn die Start-/Stopp-Dienste vom Plug-In ausgeführt werden.
  - Y, wenn Start-/\*\*Stopp-Dienste vom Benutzer ausgeführt werden.
  - Optionaler Parameter, da der Standardwert auf N gesetzt ist.
- OPLOG\_PATH\_ = (Optionaler Parameter, falls er bereits als benutzerdefiniertes Schlüssel-Wert-Paar in SnapCenter bereitgestellt wird).

### Plug-in für MaxDB

Ressourceneinstellungen:

- XUSER\_ENABLE (Y|N) aktiviert oder deaktiviert die Verwendung eines Xusers für MaxDB, sodass für den Datenbankbenutzer kein Kennwort erforderlich ist.
- HANDLE\_LOGWRITER (Y|N) führt die Operationen „Logwriter anhalten“ (N) oder „Logwriter fortsetzen“ (Y) aus.
- DBMCLICMD (path\_to\_dbmcli\_cmd) gibt den Pfad zum MaxDB-dbmcli-Befehl an. Wenn nicht festgelegt, wird dbmcli im Suchpfad verwendet.



In einer Windows-Umgebung muss der Pfad in doppelte Anführungszeichen ("...") eingeschlossen sein.

- SQLCLICMD (path\_to\_sqlcli\_cmd) gibt den Pfad zum MaxDB-SQLCLI-Befehl an. Wenn der Pfad nicht festgelegt ist, wird sqlcli auf den Suchpfad angewendet.
- MAXDB\_UPDATE\_HIST\_LOG (Y|N) weist das MaxDB-Sicherungsprogramm an, ob es das MaxDB-Verlaufsprotokoll aktualisieren soll.
- MAXDB\_CHECK\_SNAPSHOT\_DIR: Beispiel: SID1:Verzeichnis[,Verzeichnis...]; [SID2:Verzeichnis[,Verzeichnis...]] prüft, ob ein Snap Creator-Snapshot-Kopiervorgang erfolgreich ist, und stellt sicher, dass der Snapshot erstellt wird.

Dies gilt nur für NFS. Das Verzeichnis muss auf den Speicherort verweisen, der das Verzeichnis .snapshot enthält. Mehrere Verzeichnisse können in einer durch Kommas getrennten Liste enthalten sein.

In MaxDB 7.8 und späteren Versionen wird die Datenbanksicherungsanforderung im Sicherungsverlauf als „Fehlgeschlagen“ markiert.

- **MAXDB\_BACKUP\_TEMPLATES:** Gibt eine Sicherungsvorlage für jede Datenbank an.

Die Vorlage muss vorhanden sein und ein externer Typ einer Sicherungsvorlage sein. Um die Snapshot-Integration für MaxDB 7.8 und höher zu aktivieren, müssen Sie über die MaxDB-Hintergrundserverfunktionalität und eine bereits konfigurierte MaxDB-Sicherungsvorlage des Typs **EXTERNAL** verfügen.

- **MAXDB\_BG\_SERVER\_PREFIX:** Gibt das Präfix für den Hintergrundservernamen an.

Wenn der Parameter **MAXDB\_BACKUP\_TEMPLATES** festgelegt ist, müssen Sie auch den Parameter **MAXDB\_BG\_SERVER\_PREFIX** festlegen. Wenn Sie das Präfix nicht festlegen, wird der Standardwert **na\_bg\_** verwendet.

## Plug-in für SAP ASE

Ressourceneinstellungen:

- **SYBASE\_SERVER** (*data\_server\_name*) gibt den Namen des Sybase-Datenservers an (Option **-S** im **isql**-Befehl). Zum Beispiel **p\_test**.
- **SYBASE\_DATABASES\_EXCLUDE** (*db\_name*) ermöglicht das Ausschließen von Datenbanken, wenn die Konstruktion „ALL“ verwendet wird.

Sie können mehrere Datenbanken angeben, indem Sie eine durch Semikolon getrennte Liste verwenden. Beispiel: **pubs2;test\_db1**.

- **SYBASE\_USER:** *user\_name* gibt den Betriebssystembenutzer an, der den **isql**-Befehl ausführen kann.

Erforderlich für UNIX. Dieser Parameter ist erforderlich, wenn der Benutzer, der die Start- und Stoppbefehle des Snap Creator Agent ausführt (normalerweise der Root-Benutzer), und der Benutzer, der den **isql**-Befehl ausführt, unterschiedlich sind.

- **SYBASE\_TRAN\_DUMP** *db\_name:directory\_path* ermöglicht Ihnen, nach dem Erstellen eines Snapshots einen Sybase-Transaktionsdump durchzuführen. Beispiel: **pubs2:/sybasedumps/pubs2**

Sie müssen jede Datenbank angeben, die einen Transaktionsdump erfordert.

- **SYBASE\_TRAN\_DUMP\_COMPRESS** (Y|N) aktiviert oder deaktiviert die native Sybase-Transaktionsdump-Komprimierung.
- **SYBASE\_ISQL\_CMD** (z. B. **/opt/sybase/OCS-15\_0/bin/isql**) definiert den Pfad zum **isql**-Befehl.
- Mit **SYBASE\_EXCLUDE\_TEMPDB** (Y|N) können Sie vom Benutzer erstellte temporäre Datenbanken automatisch ausschließen.

## Plug-in für Oracle-Anwendungen (ORASCPM)

Ressourceneinstellungen:

- **SQLPLUS\_CMD** gibt den Pfad zu SQLplus an.
- **ORACLE\_DATABASES** listet die zu sichernden Oracle-Datenbanken und den entsprechenden Benutzer (Datenbank:Benutzer) auf.
- **CNTL\_FILE\_BACKUP\_DIR** gibt das Verzeichnis für die Sicherung der Steuerdatei an.
- **ORA\_TEMP** gibt das Verzeichnis für temporäre Dateien an.



- ORACLE\_HOME gibt das Verzeichnis an, in dem die Oracle-Software installiert ist.
- ARCHIVE\_LOG\_ONLY gibt an, ob die Archivprotokolle gesichert werden sollen oder nicht.
- ORACLE\_BACKUPMODE gibt an, ob eine Online- oder Offline-Sicherung durchgeführt werden soll.
- ORACLE\_EXPORT\_PARAMETERS gibt an, ob die oben definierten Umgebungsvariablen während der Ausführung von `/bin/su <Benutzer, der sqlplus ausführt> -c sqlplus /nolog <cmd>` erneut exportiert werden sollen. Dies ist normalerweise der Fall, wenn der Benutzer, der sqlplus ausführt, nicht alle Umgebungsvariablen festgelegt hat, die für die Verbindung mit der Datenbank mithilfe von `connect / as sysdba` erforderlich sind.

## Erstellen Sie Richtlinien für von NetApp unterstützte Plug-In-Ressourcen

Bevor Sie SnapCenter zum Sichern von Plug-in-spezifischen Ressourcen verwenden, die von NetApp unterstützt werden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten.

### Bevor Sie beginnen

- Sie sollten Ihre Sicherungsstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für von NetApp unterstützte Plug-Ins.

- Sie sollten sich auf den Datenschutz vorbereitet haben.

Zur Vorbereitung des Datenschutzes gehören Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Ressourcen.

- Die virtuellen Speichermaschinen (SVMs) sollten Ihnen für Spiegelungs- oder Tresorvorgänge zugewiesen werden.

Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

- Sie sollten die Ressourcen, die Sie schützen möchten, manuell hinzugefügt haben.

### Informationen zu diesem Vorgang

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren. Darüber hinaus können Sie Replikations-, Skript- und Anwendungseinstellungen angeben.
- Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.
- 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.



Die primären SnapLock -Einstellungen werden in der SnapCenter -Sicherungsrichtlinie verwaltet und die sekundären SnapLock -Einstellungen werden von ONTAP verwaltet.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie den Speichertyp aus.
  - b. Geben Sie im Abschnitt „Benutzerdefinierte Sicherungseinstellungen“ alle spezifischen Sicherungseinstellungen an, die im Schlüssel-Wert-Format an das Plug-In übergeben werden müssen.  
  
Sie können mehrere Schlüsselwerte angeben, die an das Plug-In übergeben werden sollen.
6. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:
  - a. Geben Sie den Zeitplantyp an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.



Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- a. Geben Sie im Abschnitt „Snapshot-Einstellungen“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherungstyp“ ausgewählt wurden:

| Wenn Sie wollen...                                                 | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behalten Sie eine bestimmte Anzahl von Snapshots                   | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> <div>  <p>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.</p> </div> <div>  <p>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.</p> </div> |
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Sperrzeitraum für Snapshot-Kopien                                  | <p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopien</b> und geben Sie Tage, Monate oder Jahre an.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

b. Wählen Sie eine 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.

7. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

| Für dieses Feld...                                                                                 | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b></p> | <p>Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation).</p> <p>Wenn die Schutzbeziehung in ONTAP vom Typ „Mirror und Vault“ ist und Sie nur diese Option auswählen, wird der auf dem primären Server erstellte Snapshot nicht zum Ziel übertragen, sondern im Ziel aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird die folgende Fehlermeldung angezeigt: „Der sekundäre Speicherort ist für die ausgewählte gewölbte/gespiegelte Sicherung nicht verfügbar.“</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“"</a> .</p> |

| Für dieses Feld...                                                                         | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben</b> | <p>Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.</p> <p>Weitere Informationen zu SnapLock Vault finden Sie unter „Snapshots an WORM auf einem Tresorziel übermitteln“.</p> <p>Sehen <a href="#">"Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“"</a> .</p> |
| <b>Fehler bei der Wiederholungsanzahl</b>                                                  | Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

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

## Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Damit können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### Schritte

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

2. Wählen Sie auf der Seite „Ressourcen“ die Option „Neue Ressourcengruppe“ aus.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | <p>Geben Sie einen Namen für die Ressourcengruppe ein.</p> <p>Hinweis: Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.</p>                                                                                                                                                                                                      |
| Schlagwörter                                                  | <p>Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.</p> <p>Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.</p>                                                                |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | <p>Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.</p> <p>Beispiel: <i>customtext_resource</i><br/> <i>group_policy_hostname</i> oder <i>resource</i><br/> <i>group_hostname</i>. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p> |

4. Optional: Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und den Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

Dies hilft, Informationen auf dem Bildschirm zu filtern.

5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Optional: Gehen Sie auf der Seite **Anwendungseinstellungen** wie folgt vor:

- a. Wählen Sie den Pfeil „Backups“ aus, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Consistency Group Snapshot-Vorgangs zu warten | <p>Wählen Sie „Dringend“, „Mittel“ oder „Entspannt“ aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs festzulegen.</p> <p>Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.</p> |

| Für dieses Feld...                  | Machen Sie Folgendes...                                                             |
|-------------------------------------|-------------------------------------------------------------------------------------|
| WAFL -Synchronisierung deaktivieren | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden. |

+

- 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 den Pfeil „Benutzerdefinierte Konfigurationen“ aus und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

| Parameter            | Einstellung                | Beschreibung                                                                                                                                                     |
|----------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIV_LOG_ENABLE    | (J/N)                      | Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle.                                                                                        |
| ARCHIV_LOG_RETENTION | Anzahl_der_Tage            | Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden.<br><br>Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein. |
| ARCHIVE_LOG_DIR      | change_info_directory/logs | Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.                                                                                              |

| Parameter                     | Einstellung      | Beschreibung                                                                                                                                                                                                                                                   |
|-------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARCHIVE_LOG_EXT               | Dateierweiterung | Gibt die Erweiterungslänge der Archivprotokolldatei an.<br><br>Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.16151855 1942 9 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (J/N)            | Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen.<br><br>Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.                                                                         |

c. Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                                                                        | Dann...                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar. | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.<br><br>Diese Option ist für das SnapCenter -Plug-in für die SAP HANA-Datenbank nicht anwendbar. |
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                                                                                    | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                                                                                |
| Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshots zu erstellen.                                                                                                                 | Wählen Sie <b>Andere</b> aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen.            |

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

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



Sie können auch eine Richtlinie erstellen, indem Sie \* auswählen. \*.

Die Richtlinien sind im Abschnitt **Zeitpläne für ausgewählte Richtlinien konfigurieren** aufgeführt.

b. Wählen Sie in der Spalte **Zeitpläne konfigurieren** \* \* für die Richtlinie, die Sie konfigurieren möchten.



- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen*“ den Zeitplan und wählen Sie „OK“ aus.

Dabei ist „Richtliniennamen“ 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 aus der Dropdown-Liste **E-Mail-Einstellungen** auf der Seite **Benachrichtigung** 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. Der SMTP-Server muss unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

9. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

## Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Ressourcen 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                                                                         |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> .                                                        |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ angegeben haben.

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Ausführen von Datenschutzvorgängen verwenden.

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Verwaltungs-LIF-IP-Adresse haben.

### Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets `Open-SmConnection`.

Dieses Beispiel öffnet eine PowerShell-Sitzung:

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie mithilfe des Cmdlets `Add-SmStorageConnection` eine neue Verbindung zum Speichersystem.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Erstellen Sie mithilfe des Cmdlets `Add-SmCredential` neue Anmeldeinformationen.

In diesem Beispiel wird eine neue Anmeldeinformation mit dem Namen „FinanceAdmin“ mit Windows-Anmeldeinformationen erstellt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

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"](#) .

## **Sichern Sie einzelne von NetApp unterstützte Plug-In-Ressourcen**

Wenn eine einzelne von NetApp unterstützte Plug-In-Ressource nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern. Sie können die Ressource bei Bedarf sichern. Wenn für die Ressource eine Richtlinie festgelegt und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### **Bevor Sie beginnen**

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Klicken  und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auf , um den Filterbereich zu schließen.

3. Klicken Sie auf die Ressource, die Sie sichern möchten.
4. Wenn Sie auf der Ressourcenseite einen benutzerdefinierten Namen verwenden möchten, aktivieren Sie das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** und geben Sie dann ein benutzerdefiniertes Namensformat für den Snapshot-Namen ein.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

- a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

| Für dieses Feld...                                                                          | Machen Sie Folgendes...                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Planen Sie Zeit ein, um auf den Abschluss des Consistency Group Snapshot-Vorgangs zu warten | <p>Wählen Sie „Dringend“, „Mittel“ oder „Entspannt“ aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs festzulegen.</p> <p>Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.</p> |
| WAFL -Synchronisierung deaktivieren                                                         | Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.                                                                                                                               |

+

- a. Klicken Sie auf den Pfeil **Skripts**, um Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen. Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen.

Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

- b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

| Falls Sie es wollen...                                                                                                                                   | Dann...                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| SnapCenter zum Erstellen eines Snapshots auf Speicherebene                                                                                               | Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.                                      |
| SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen | Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.                                       |
| So geben Sie den Befehl zum Erstellen eines Snapshots ein                                                                                                | Wählen Sie <b>Andere</b> und geben Sie dann den Befehl zum Erstellen eines Snapshots ein. |

6. 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.  in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamenname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

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

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

Die Seite mit der Ressourcentopologie wird angezeigt.

9. Klicken Sie auf **Jetzt sichern**.

10. 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**.

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

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146\
```

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Fügen Sie Ressourcen mithilfe des Cmdlets Add-SmResources hinzu.

In diesem Beispiel werden Ressourcen hinzugefügt:



```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QTREEName"="qtree
Voll1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

### 3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

In diesem Beispiel wird eine neue Sicherungsrichtlinie erstellt:

```
Add-SmPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

### 4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

In diesem Beispiel wird eine neue Ressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

### 5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

```
New-SmBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

### 6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

In diesem Beispiel wird ein Job-Zusammenfassungsbericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
Get-SmBackupReport -JobId 149
```

```
BackedUpObjects      : {QTREE2, QTREE}
FailedObjects        : {}
IsScheduled          : False
HasMetadata          : False
SmBackupId           : 1
SmJobId              : 149
StartDateTime        : 1/15/2024 1:35:17 AM
EndDateTime          : 1/15/2024 1:36:19 AM
Duration             : 00:01:02.4265750
CreatedDateTime      : 1/15/2024 1:35:51 AM
Status               : Completed
ProtectionGroupName  :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId  : 1
PolicyName           : test2
SmPolicyId           : 4
BackupName           :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError           :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : DummyPlugin
PluginDisplayName     : DummyPlugin
JobTypeId            :
JobHost              : scc55.sscore.test.com
```

## Sichern Sie Ressourcengruppen von NetApp unterstützten Plug-In-Ressourcen

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror -Beziehung zum sekundären Speicher sichern möchten, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn

Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

## 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 „Anzeigen“ die Option „Ressourcengruppe“ aus.

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf  und wählen Sie das Tag aus. Sie können dann auf , um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
  - a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet 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**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.
    - In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

"SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl. Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei /opt/netapp/init\_scripts/scvservice. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`.

## Überwachen Sie die Sicherungsvorgänge für NetApp unterstützte Plug-In-Ressourcen

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.

## Abbrechen von Sicherungsvorgängen für von NetApp unterstützte Plug-Ins

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzuberechnen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

| Von der...        | Aktion                                                                                                                                                                                                                                                                                                                                         |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitorseite      | <p>a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b>.</p> <p>b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b>.</p>                                                                                                                                                                       |
| Aktivitätsbereich | <p>a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf ** im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.</p> <p>b. Wählen Sie den Vorgang aus.</p> <p>c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b>.</p> |

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

## Anzeigen von ressourcenbezogenen Backups und Klonen von NetApp unterstützten Plug-ins auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzuzeigen. Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

### Informationen zu diesem Vorgang

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.



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.

•



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.

## 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 die Anwendungsressource auf 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.

Nach der On-Demand-Sicherung werden durch Klicken auf die Schaltfläche **Aktualisieren** die Details der Sicherung oder des Klons aktualisiert.

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-, Umbenennungs- und Löschvorgänge durchzuführen.



Sie können Sicherungen, die sich auf dem sekundären Speichersystem befinden, weder umbenennen noch löschen.



Sie können die Sicherungen, die sich auf dem primären Speichersystem befinden, nicht umbenennen.

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

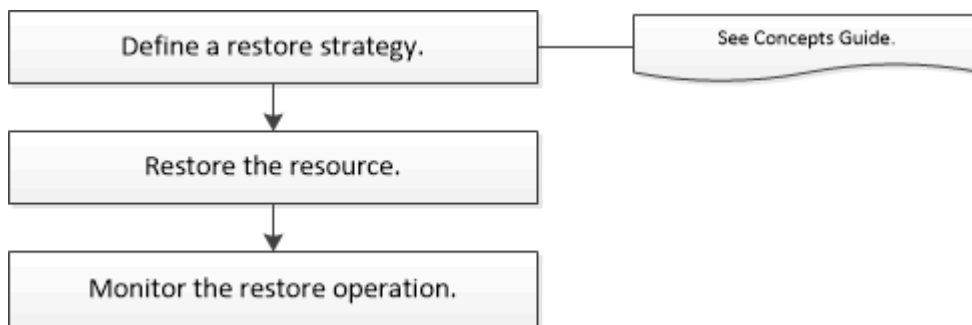
## Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen

### Wiederherstellen von NetApp -unterstützten Plug-In-Ressourcen

Der Wiederherstellungs-Workflow umfasst die Planung und Durchführung der Wiederherstellungsvorgänge sowie die Überwachung der Vorgänge.

#### Informationen zu diesem Vorgang

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Informationen zu PowerShell-Cmdlets finden Sie in der Hilfe zu SnapCenter -Cmdlets oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

### Wiederherstellen einer Ressourcensicherung

Sie können SnapCenter zum Wiederherstellen von Ressourcen verwenden. Die Möglichkeiten der Wiederherstellungsvorgänge hängen vom verwendeten Plug-In ab.

#### Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Sie müssen alle derzeit laufenden Sicherungsvorgänge für die Ressource oder Ressourcengruppe, die Sie wiederherstellen möchten, abgebrochen haben.

#### Informationen zu diesem Vorgang

- Der Standardwiederherstellungsvorgang stellt nur Speicherobjekte wieder her. Wiederherstellungsvorgänge auf Anwendungsebene können nur durchgeführt werden, wenn das von NetApp unterstützte Plug-In diese Funktion bietet.

- 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.



## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Informationen wie Typ, Host- oder Clustername, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.



Obwohl eine Sicherung möglicherweise für eine Ressourcengruppe erfolgt, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die Sie wiederherstellen möchten.

Wenn die Ressource nicht geschützt ist, wird in der Spalte **Gesamtstatus** *Nicht geschützt* angezeigt.

Der Status *Nicht geschützt* in der Spalte **Gesamtstatus** kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource von einem anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Kopien verwalten** die Option **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf .

| Primary Backup(s)                           |                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| search                                      |                        |
| Backup Name                                 | End Date                                                                                                  |
| rg1_scpr0191685001_01-05-2017_01.35.06.6463 | 1/5/2017 1:35:27 AM  |

6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ entweder **Vollständige Ressource** oder **Dateiebene** aus.

- a. Wenn Sie **Ressource vervollständigen** ausgewählt haben, wird die Ressourcensicherung wiederhergestellt.

Wenn die Ressource Volumes oder Qtrees als Speicherbedarf enthält, werden neuere Snapshots auf solchen Volumes oder Qtrees gelöscht und können nicht wiederhergestellt werden. Wenn eine andere Ressource auf denselben Volumes oder Qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

- b. Wenn Sie **Dateiebene** ausgewählt haben, können Sie entweder **Alle** auswählen oder Volumes oder Qtrees auswählen und dann den Pfad zu den ausgewählten Volumes oder Qtrees durch Kommas getrennt eingeben.

- Sie können mehrere Volumes und Qtrees auswählen.
- Wenn der Ressourcentyp LUN ist, wird die gesamte LUN wiederhergestellt. Sie können mehrere LUNs auswählen. + HINWEIS: Wenn Sie **Alle** auswählen, werden alle Dateien auf den Volumes, Qtrees oder LUNs wiederhergestellt.

7. Geben Sie auf der Seite **Pre ops** die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
8. Geben Sie auf der Seite **Post Ops** Mount- und Post Restore-Befehle ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
9. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## PowerShell-Cmdlets

### Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime | BackupType |
|----------|-------------------------------|------------|------------|
| -----    | -----                         | -----      | -----      |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:02:32   |
| AM       | Full Backup                   |            |            |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015   | 11:23:17   |
| AM       |                               |            |            |

Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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"](#) .

## Überwachen Sie die Wiederherstellungsvorgänge für von NetApp unterstützte Plug-In-Ressourcen

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 NetApp -unterstützte Plug-In-Ressourcensicherungen

### Klonen Sie NetApp -unterstützte Plug-In-Ressourcensicherungen

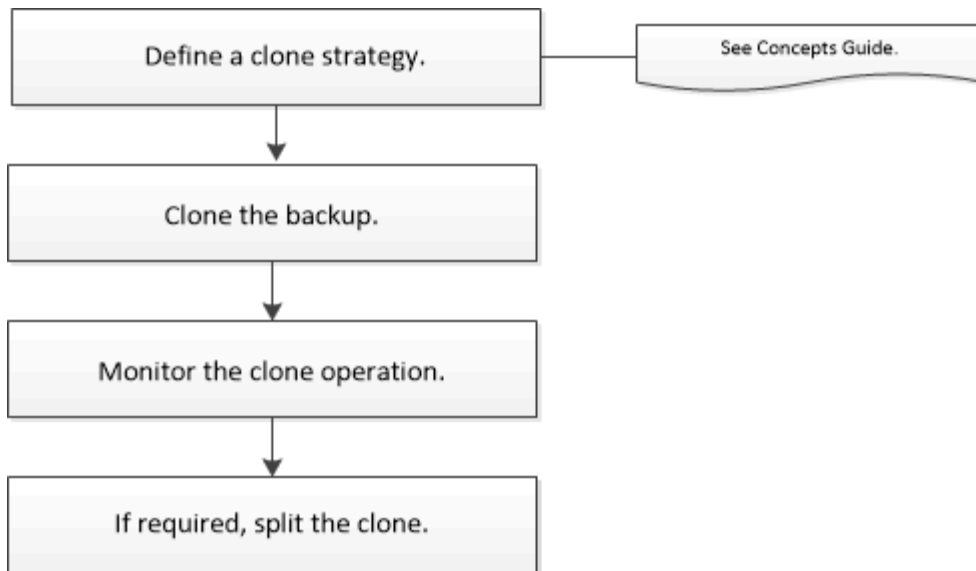
Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

#### Informationen zu diesem Vorgang

Sie können Ressourcensicherungen aus den folgenden Gründen klonen:

- Zum Testen von Funktionen, die während der Anwendungsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
- Für Datenextraktions- und Manipulationstools beim Befüllen von Data Warehouses
- So stellen Sie versehentlich gelöschte oder geänderte Daten wieder her

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Klonvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Klonen aus einer Sicherung

Sie können SnapCenter verwenden, um ein Backup zu klonen. Sie können von einer primären oder sekundären Sicherung klonen. Die Möglichkeiten der Klonvorgänge hängen vom verwendeten Plug-In ab.

### Bevor Sie beginnen

- Sie müssen die Ressourcen oder Ressourcengruppe gesichert haben.
- Der Standardklonvorgang kloniert nur Speicherobjekte. Klonvorgänge auf Anwendungsebene können nur durchgeführt werden, wenn das von NetApp unterstützte Plug-In diese Funktion bietet.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.

### Informationen zu diesem Vorgang

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.

## SnapCenter -Benutzeroberfläche

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite **Ressourcen** die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

Die Ressourcen werden zusammen mit Informationen wie Typ, Host- oder Clustername, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standorte“ die folgenden Schritte aus:

| Für dieses Feld... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server klonen      | <p>Standardmäßig ist der Quellhost ausgefüllt.</p> <p>Wenn Sie einen anderen Host angeben möchten, wählen Sie den Host aus, auf dem der Klon gemountet und das Plug-In installiert werden soll.</p>                                                                                                                                                                                                                                                                                                          |
| Klonsuffix         | <p>Dies ist obligatorisch, wenn das Klonziel mit der Quelle identisch ist.</p> <p>Geben Sie ein Suffix ein, das an den neu geklonten Ressourcennamen angehängt wird. Das Suffix stellt sicher, dass die geklonte Ressource auf dem Host eindeutig ist.</p> <p>Beispiel: rs1_clone. Wenn Sie auf denselben Host wie die ursprüngliche Ressource klonen, müssen Sie ein Suffix angeben, um die geklonte Ressource von der ursprünglichen Ressource zu unterscheiden. Andernfalls schlägt der Vorgang fehl.</p> |

Wenn es sich bei der ausgewählten Ressource um eine LUN handelt und Sie von einer sekundären Sicherung klonen, werden die Zielvolumes aufgelistet. Eine einzelne Quelle kann mehrere Zielvolumes haben.

7. Führen Sie auf der Seite **Einstellungen** Folgendes aus:

| Für dieses Feld...  | Machen Sie Folgendes...                                                         |
|---------------------|---------------------------------------------------------------------------------|
| Name des Initiators | Geben Sie den Host-Initiatornamen ein, der entweder ein IQDN oder ein WWPN ist. |
| Igroup-Protokoll    | Wählen Sie das Igroup-Protokoll.                                                |



Die Einstellungsseite wird nur angezeigt, wenn der Speichertyp LUN ist.

- Geben Sie auf der Seite „Skripte“ die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Beispiel:

- Befehl vor dem Klonen: Löschen Sie vorhandene Datenbanken mit demselben Namen
- Befehl nach dem Klonen: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.

Mount-Befehl für ein Volume oder einen Qtree auf einer Linux-Maschine:

`mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>`

- Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **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.

- Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.
- Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## PowerShell-Cmdlets

### Schritte

- Initiieren Sie mithilfe des Cmdlets `Open-SmConnection` eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- Listen Sie die Sicherungen auf, die mit dem Cmdlet `Get-SmBackup` oder `Get-SmResourceGroup` geklont werden können.

Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:



```
C:\PS>PS C:\> Get-SmBackup
```

| BackupId | BackupName                    | BackupTime           | BackupType  |
|----------|-------------------------------|----------------------|-------------|
| -----    | -----                         | -----                | -----       |
| 1        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:02:32 AM | Full Backup |
| 2        | Payroll Dataset_vise-f6_08... | 8/4/2015 11:23:17 AM |             |

In diesem Beispiel werden Informationen zu einer angegebenen Ressourcengruppe angezeigt:

```
PS C:\> Get-SmResourceGroup
```

```
Description :
CreationTime : 10/10/2016 4:45:53 PM
ModificationTime : 10/10/2016 4:45:53 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {}
HostResourceMapping : {}
Configuration :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus : Completed
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Tag :
IsInternal : False
```

```

EnableEmailAttachment      : False
VerificationSettings       : {}
Name                       : NFS_DB
Type                       : Group
Id                         : 2
Host                      :
UserName                  :
Passphrase                 :
Deleted                   : False
Auth                      : SMCoreContracts.SmAuth
IsClone                   : False
CloneLevel                : 0
Hosts                     :
StorageName               :
ResourceGroupNames        :
PolicyNames               :

Description                :
CreationTime               : 10/10/2016 4:51:36 PM
ModificationTime           : 10/10/2016 5:27:57 PM
EnableEmail                : False
EmailSMTPServer            :
EmailFrom                  :
EmailTo                    :
EmailSubject               :
EnableSysLog               : False
ProtectionGroupType        : Backup
EnableAsupOnFailure        : False
Policies                   : {}
HostResourceMapping        : {}
Configuration              :
SMCoreContracts.SmCloneConfiguration
  LastBackupStatus         : Failed
  VerificationServer        :
  EmailBody                 :
  EmailNotificationPreference : Never
  VerificationServerInfo    :
  SchedulerSQLInstance      :
  CustomText                :
  CustomSnapshotFormat      :
  SearchResources           : False
  ByPassRunAs               : False
  IsCustomSnapshot          :
  MaintenanceStatus         : Production
  PluginProtectionGroupTypes : {SMSQL}
  Tag                       :

```

```

IsInternal           : False
EnableEmailAttachment : False
VerificationSettings : {}
Name                 : Test
Type                 : Group
Id                   : 3
Host                 :
UserName             :
Passphrase           :
Deleted              : False
Auth                 : SMCoreContracts.SmAuth
IsClone              : False
CloneLevel           : 0
Hosts                :
StorageName          :
ResourceGroupNames   :
PolicyNames          :

```

3. Starten Sie mit dem Cmdlet `New-SmClone` einen Klonvorgang aus einer Klonressourcengruppe oder einer vorhandenen Sicherung.

Dieses Beispiel erstellt einen Klon aus einem angegebenen Backup mit allen Protokollen:

```

New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'

```

4. Zeigen Sie den Status des Klonauftrags mithilfe des Cmdlets `Get-SmCloneReport` an.

Dieses Beispiel zeigt einen Klonbericht für die angegebene Job-ID an:

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId             : 186
StartDateTime       : 8/3/2015 2:43:02 PM
EndDateTime        : 8/3/2015 2:44:08 PM
Duration            : 00:01:06.6760000
Status              : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName          : OnDemand_Clone
SmPolicyId          : 4
BackupPolicyName    : OnDemand_Full_Log
SmBackupPolicyId    : 1
CloneHostName       : SCSPR0054212005.mycompany.com
CloneHostId        : 4
CloneName           : Draper__clone__08-03-2015_14.43.53
SourceResources     : {Don, Betty, Bobby, Sally}
ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError          :
```

## Überwachen Sie von NetApp unterstützte Plug-in-Ressourcenklonvorgänge

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**.

# 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      | <ul style="list-style-type: none"><li>• Physischer Server</li><li>• Virtueller Server</li></ul> <p>vVol-Datenspeicher auf NFS und SAN. vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.</p>      |
| Betriebssysteme | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• SUSE Linux Enterprise Server (SLES)</li></ul>                                                                                         |
| Dateisysteme    | <ul style="list-style-type: none"><li>• SAN:<ul style="list-style-type: none"><li>◦ Sowohl LVM- als auch nicht LVM-basierte Dateisysteme</li><li>◦ LVM über VMDK ext3, ext4 und xfs</li></ul></li><li>• NFS: NFS v3, NFS v4.x</li></ul> |
| Protokolle      | <ul style="list-style-type: none"><li>• FC</li><li>• FCoE</li><li>• iSCSI</li><li>• NFS</li></ul>                                                                                                                                       |

| 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                                                                              | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• SUSE Linux Enterprise Server (SLES)</li></ul>                                                                                                                                                                                                                                                                         |
| Mindest-RAM für das SnapCenter -Plug-In auf dem Host                                         | 2 GB                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host | <div><div>2 GB</div><div> 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.</div></div> |



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

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 <b>Linux</b> als Hosttyp.                                                                                                                                                                                                                                                                                                                     |
| Hostname           | <p>Geben Sie den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.</p> <p>SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben.</p> <p>Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.</p> |

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

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              | <p>Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an.</p> <p>Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt.</p> <div>  <p>Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.</p> </div> |
| Installationspfad  | <p>Der Standardpfad ist <i>/opt/NetApp/snapcenter</i>.</p> <p>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.</p>                                                                                                                                                                                                                                                                                  |

| 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     | <p>Zeigt die unterstützten Protokollebenen an.</p> <p>Die möglichen Werte sind TRACE, DEBUG, INFO, WARN, ERROR und FATAL.</p> |

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

| Parametername                           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOGS_MAX_COUNT                          | <p>Zeigt die Anzahl der Protokolldateien des SnapCenter Plug-in Loader an, die im Ordner <code>/custom_location/snapcenter/spl/logs</code> gespeichert sind.</p> <p>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.</p> <div>  <p>Wenn Sie die Datei „spl.properties“ manuell löschen, wird die Anzahl der beizubehaltenden Dateien auf 9999 festgelegt.</p> </div> |
| JAVA_HOME                               | <p>Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird.</p> <p>Dieser Pfad wird während der Installation und beim Starten von SPL festgelegt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| LOG_MAX_SIZE                            | <p>Zeigt die maximale Größe der Job-Protokolldatei an.</p> <p>Sobald die maximale Größe erreicht ist, wird die Protokolldatei komprimiert und die Protokolle in die neue Datei dieses Auftrags geschrieben.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Protokolle der letzten Tage aufbewahren | <p>Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Zertifikatsvalidierung aktivieren       | <p>Zeigt „true“ an, wenn die CA-Zertifikatsvalidierung für den Host aktiviert ist.</p> <p>Sie können diesen Parameter entweder durch Bearbeiten der spl.properties oder mithilfe der SnapCenter -GUI oder des Cmdlets aktivieren oder deaktivieren.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |

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
<AliasNameForCertificateToBeImported> -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 Schlüsselspeicherkenwort.

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 "<OriginalAliasName>" -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 Sicherungstypeneinstellungen 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 | <p>Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation).</p> <p>Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.</p> |

| 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                   | <p>Wählen Sie <b>Zu behaltende Kopien</b> und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten.</p> <p>Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p> <div>  <p>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.</p> </div> <div>  <p>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.</p> </div> |
| Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf | Wählen Sie <b>Kopien aufbewahren für</b> und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                   |                                                                                                                                                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sperrzeitraum für Snapshot-Kopien | <p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopien</b> und geben Sie die Dauer in Tagen, Monaten oder Jahren an.</p> <p>Die Aufbewahrungsdauer von Snaplock sollte weniger als 100 Jahre betragen.</p> |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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

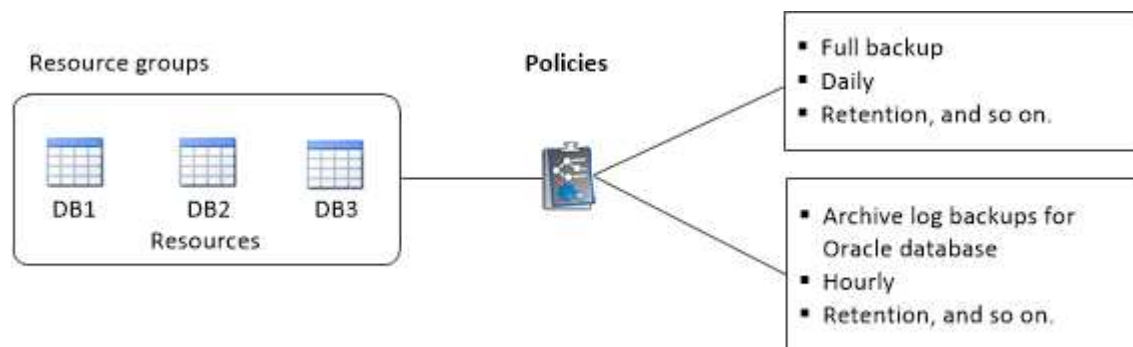
Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle mit den Dateisystemen verknüpften Daten sichern.

### 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.  in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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-SmSmtServer“ 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 *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist *Richtliniennamen* 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“ (Richtliniennamen) die folgenden Aktionen aus:

| Wenn Sie wollen...                                   | Machen Sie Folgendes...                                                                                         |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Führen Sie nach der Sicherung eine Überprüfung durch | Wählen Sie <b>Überprüfung nach Sicherung ausführen</b> .                                                        |
| Planen Sie eine Überprüfung                          | Wählen Sie <b>Geplante Überprüfung ausführen</b> 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-SmSmtServer“ 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 Sie  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 *Richtliniennamen* 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-SmSmtServer` .

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-SmSmtServer“ 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-SmSmtServer“ 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 <b>Datenbank</b> aus der Ansichtsliste. |
| Für Dateisysteme         | Wählen Sie <b>Pfad</b> 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**.



# Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden

## Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden

SnapCenter unterstützt den Schutz Ihrer Anwendungen wie Oracle, SQL und SAP HANA, die sich auf Azure NetApp Files befinden. Ab Version 6.0.1 unterstützt SnapCenter die Azure NetApp Files -Sicherungsfunktion, die die Datenschutzfunktionen von Azure NetApp Files erweitert, indem sie eine vollständig verwaltete Sicherungslösung für langfristige Wiederherstellung, Archivierung und Compliance bietet.

Azure NetApp Files ist eine Premium-Speicherlösung, deren langfristige Aufbewahrung von Backups teuer sein kann. Um die Kosten zu optimieren, können Sie die Sicherungen vom Azure NetApp Files -Speicher in einen Azure-Objektspeicher verschieben. Ab SnapCenter 6.0.1 können Sie Anwendungen, die sich auf Azure NetApp Files befinden, in Azure Blob Storage (Objektspeicher) sichern und klonen. Sie können zwei Kopien Ihrer Daten aufbewahren: Volume-Snapshot-Kopien im Azure NetApp Files -Speicher für die kurzfristige Wiederherstellung und eine weitere Kopie im Azure Blob Storage für die langfristige Wiederherstellung.

Wenn eine Richtlinie mit Azure NetApp Files -Sicherung aktiviert und einer Ressource zugeordnet ist, übernimmt SnapCenter die Erstellung von Volume-Snapshots und deren Sicherung in Azure Blob Storage. SnapCenter erstellt den Backup-Tresor und aktiviert die Sicherung für das Volume. Wenn Sie die Sicherung für das Volume aktiviert haben, verwendet SnapCenter den vorhandenen Tresor.

### Einschränkungen

- Objektspeicherfunktionen für FAS, ASA oder AFF ONTAP und Amazon FSx for NetApp ONTAP Speichersysteme werden nicht unterstützt.
- Mount- und Katalog-Workflows von Oracle und SAP HANA werden für Objektspeicher-Backups nicht unterstützt, für Snapshots jedoch schon.
- Oracle PDB-Klone werden für Objektspeichersicherungen nicht unterstützt, für Snapshots jedoch schon.
- Die Sicherungsüberprüfung aus dem Objektspeicher, die REST-API-Unterstützung, die Verwaltung des Klon-Lebenszyklus aus dem Objektspeicher und die Berichtsfunktionen für Objektspeicher-Sicherungen werden nicht unterstützt.
- Die Wiederherstellung von Sicherungen auf Azure Blob Storage in Azure NetApp Files wird nicht unterstützt. Alternativ können Sie die Klonoption verwenden.
- Klonaufteilung wird nicht unterstützt.

## Installieren Sie SnapCenter und erstellen Sie Anmeldeinformationen

### Installieren von SnapCenter auf einer virtuellen Azure-Maschine

Sie können die SnapCenter software von der NetApp -Support-Site herunterladen und die Software auf der virtuellen Azure-Maschine installieren.

## Bevor Sie beginnen

- Stellen Sie sicher, dass die virtuelle Azure Windows-Maschine die Anforderungen für die Installation von SnapCenter Server erfüllt. Weitere Informationen finden Sie unter "[Voraussetzungen für die Installation von SnapCenter Server](#)".
- Wenn Sie Azure NetApp Files noch nicht kennen und noch kein NetApp -Konto haben, stellen Sie sicher, dass Sie sich registriert haben, damit Sie auf die SnapCenter -Software zugreifen können. Weitere Informationen finden Sie unter "[Registrieren Sie sich, um auf die SnapCenter software zuzugreifen](#)".

## Schritte

1. Laden Sie das SnapCenter Server-Installationspaket herunter von "[NetApp Support Site](#)".
2. Starten Sie die Installation des SnapCenter -Servers, indem Sie auf die heruntergeladene EXE-Datei doppelklicken.

Nachdem Sie die Installation gestartet haben, werden alle Vorprüfungen durchgeführt und wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen angezeigt. Sie können die Warnmeldungen ignorieren und mit der Installation fortfahren. Fehler sollten jedoch behoben sein.

3. Überprüfen Sie die vorab ausgefüllten Werte, die für die Installation des SnapCenter -Servers erforderlich sind, und ändern Sie sie bei Bedarf.

Sie müssen das Kennwort für die MySQL Server-Repository-Datenbank nicht angeben. Während der Installation des SnapCenter -Servers wird das Kennwort automatisch generiert.



Das Sonderzeichen „%“ wird im benutzerdefinierten Pfad für die Repository-Datenbank nicht unterstützt. Wenn Sie „%“ in den Pfad aufnehmen, schlägt die Installation fehl.

4. Klicken Sie auf **Jetzt installieren**.

Sollten Sie ungültige Werte angegeben haben, werden entsprechende Fehlermeldungen angezeigt. Sie sollten die Werte erneut eingeben und dann die Installation starten.



Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wird der ausgeführte Schritt abgeschlossen und anschließend der Rollback-Vorgang gestartet. Der SnapCenter -Server wird vollständig vom Host entfernt.

Wenn Sie jedoch auf **Abbrechen** klicken, während die Vorgänge „Neustart der SnapCenter Server-Site“ oder „Warten auf den Start des SnapCenter Servers“ ausgeführt werden, wird die Installation fortgesetzt, ohne den Vorgang abubrechen.

## Registrieren Sie das Produkt, um den Support zu aktivieren

Wenn Sie neu bei NetApp sind und noch kein NetApp -Konto haben, sollten Sie das Produkt registrieren, um Support zu erhalten.

## Schritte

1. Navigieren Sie nach der Installation von SnapCenter zu **Hilfe > Info**.
2. Notieren Sie sich im Dialogfeld „Über SnapCenter“ die SnapCenter Instanz, eine 20-stellige Nummer, die mit 971 beginnt.
3. Klicken <https://register.netapp.com>.

4. Klicken Sie auf **Ich bin kein registrierter NetApp -Kunde**.
5. Geben Sie Ihre Daten ein, um sich zu registrieren.
6. Lassen Sie das Feld „NetApp -Referenz-SN“ leer.
7. Wählen Sie \* SnapCenter\* aus der Dropdown-Liste „Produktlinie“ aus.
8. Wählen Sie den Abrechnungsanbieter aus.
9. Geben Sie die 20-stellige SnapCenter Instanz-ID ein.
10. Klicken Sie auf **Senden**.

## Erstellen der Azure-Anmeldeinformationen in SnapCenter

Sie sollten die Azure-Anmeldeinformationen in SnapCenter erstellen, um auf das Azure NetApp -Konto zuzugreifen.

### Bevor Sie beginnen

- Stellen Sie sicher, dass Sie den Dienstprinzipal in Azure erstellt haben.
- Stellen Sie sicher, dass Sie über die Mandanten-ID, die Client-ID und den geheimen Schlüssel verfügen, die mit dem Dienstprinzipal verknüpft sind.
  - Die Mandanten-ID finden Sie im Azure-Portal auf der Übersichtsseite für die Entra-ID.
  - Die Client-ID wird auch als Anwendungs-ID für den Enterprise-App-/Service-Principal bezeichnet. Dies finden Sie im Azure-Portal auf der Übersichtsseite für die Unternehmensanwendung, die Sie als Dienstprinzipal für SnapCenter erstellt haben.
  - Der geheime Clientschlüssel wird auch als geheimer Wert bezeichnet. Sie können dieses Clientgeheimnis im Azure-Portal erstellen, indem Sie unter Entra ID zu **App-Registrierungen** navigieren. Nachdem Sie die von Ihnen erstellte Enterprise-App ausgewählt haben, navigieren Sie zu **Zertifikate und Geheimnisse** und dann zu **Neues Client-Geheimnis**.



Auf den geheimen Wert kann nur zugegriffen werden, wenn er erstellt wurde. Sie können später nicht mehr darauf zugreifen.

- Dem Dienstprinzipal müssen Berechtigungen erteilt werden. Die Rolle des Mitwirkenden ermöglicht dem Dienstprinzipal, erforderliche Aktionen in Azure auszuführen. Dies kann über die Zugriffssteuerungsseite (IAM) auf der Abonnementseite gewährt werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die folgenden Informationen an, die zum Erstellen der Anmeldeinformationen erforderlich sind.

| Für dieses Feld...      | Machen Sie Folgendes...                                 |
|-------------------------|---------------------------------------------------------|
| Anmeldeinformationsname | Geben Sie einen Namen für die Anmeldeinformationen ein. |

| Für dieses Feld...       | Machen Sie Folgendes...                                                 |
|--------------------------|-------------------------------------------------------------------------|
| Authentifizierungsmodus  | Wählen Sie <b>Azure-Anmeldeinformationen</b> aus der Dropdownliste aus. |
| Mandanten-ID             | Geben Sie die Mandanten-ID ein.                                         |
| Client-ID                | Geben Sie die Client-ID ein.                                            |
| Geheimer Clientschlüssel | Geben Sie den geheimen Clientschlüssel ein.                             |

5. Klicken Sie auf **OK**.

## Konfigurieren des Azure-Speicherkontos

Sie sollten das Azure-Speicherkonto in SnapCenter konfigurieren.

Das Azure-Speicherkonto enthält Details zur Abonnement-ID, den Azure-Anmeldeinformationen und dem Azure NetApp -Konto.



Die Standardlizenzen und die kapazitätsbasierte Lizenz sind für Azure NetApp Files nicht erforderlich.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Wählen Sie auf der Seite „Speichersysteme“ \* Azure NetApp Files\* aus und klicken Sie auf **Neu**.
3. Wählen Sie die Anmeldeinformationen, die Abonnement-ID und das NetApp -Konto aus den jeweiligen Dropdown-Listen aus.
4. Klicken Sie auf **Senden**.

## Erstellen Sie die Anmeldeinformationen zum Hinzufügen des Plug-In-Hosts

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren.

Sie sollten Anmeldeinformationen für die Installation von SnapCenter Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen erstellen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die folgenden Informationen an, die zum Erstellen der Anmeldeinformationen erforderlich sind.

| Für dieses Feld...                | Machen Sie Folgendes...                                                                                                                                                                                                                                                                      |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anmeldeinformationsname           | Geben Sie einen Namen für die Anmeldeinformationen ein.                                                                                                                                                                                                                                      |
| Authentifizierungsmodus           | Wählen Sie den Authentifizierungsmodus aus der Dropdown-Liste aus.                                                                                                                                                                                                                           |
| Authentifizierungstyp             | Wählen Sie entweder <b>Passwortbasiert</b> oder <b>SSH-Schlüsselbasiert</b> (nur für Linux-Host).                                                                                                                                                                                            |
| Benutzername                      | Geben Sie den Benutzernamen an.                                                                                                                                                                                                                                                              |
| Passwort                          | Wenn Sie die kennwortbasierte Authentifizierung ausgewählt haben, geben Sie das Kennwort an.                                                                                                                                                                                                 |
| Privater SSH-Schlüssel            | Wenn Sie die SSH-Schlüssel-basierte Authentifizierung ausgewählt haben, geben Sie den privaten Schlüssel an.                                                                                                                                                                                 |
| Verwenden Sie Sudo-Berechtigungen | <p>Aktivieren Sie das Kontrollkästchen „Sudo-Berechtigungen verwenden“, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.</p> <div>  <p>Dies gilt nur für Linux-Benutzer.</p> </div> |

5. Klicken Sie auf **OK**.

## Schützen Sie SAP HANA-Datenbanken

### Hosts hinzufügen und SnapCenter Plug-In für SAP HANA-Datenbank installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

#### Bevor Sie beginnen

- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Wenn Sie die Installation auf dem zentralen Host durchführen, stellen Sie sicher, dass die SAP HANA-Clientsoftware auf diesem Host installiert ist, und öffnen Sie die erforderlichen Ports auf dem SAP HANA-Datenbankhost, um die HDB-SQL-Abfragen remote auszuführen.

#### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:
  - a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
  - b. Geben Sie im Feld „Hostname“ den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.
  - c. Geben Sie im Feld „Anmeldeinformationen“ die von Ihnen erstellten Anmeldeinformationen ein.
5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Klicken Sie auf **Senden**.
8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.

9. Überwachen Sie den Installationsfortschritt.

## SAP HANA-Datenbank hinzufügen

Sie sollten die SAP HANA-Datenbank manuell hinzufügen.

### Informationen zu diesem Vorgang

Ressourcen müssen manuell hinzugefügt werden, wenn das Plug-in auf einem zentralen Server installiert ist. Wenn das SAP HANA-Plug-In auf dem HANA-Datenbankhost installiert ist, wird das HANA-System automatisch erkannt.



Die automatische Erkennung wird für die HANA-Multihostkonfiguration nicht unterstützt. Sie muss nur über ein zentrales Plug-In hinzugefügt werden.

### Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter -Plug-in für die SAP HANA-Datenbank aus der Dropdown-Liste aus und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite „Ressourcen“ auf **SAP HANA-Datenbank hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:
  - a. Geben Sie den Ressourcentyp entweder als Einzelcontainer, Multitenant-Datenbankcontainer oder Nicht-Datenvolume ein.
  - b. Geben Sie den SAP HANA-Systemnamen ein.
  - c. Geben Sie die System-ID (SID) ein.
  - d. Wählen Sie den Plug-In-Host aus.
  - e. Geben Sie den Schlüssel ein, um eine Verbindung zum SAP HANA-System herzustellen.
  - f. Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist.
4. Wählen Sie auf der Seite „Speicherbedarf angeben“ als Speichertyp „Azure NetApp Files“ aus.
  - a. Wählen Sie das Azure NetApp Konto aus.

- b. Wählen Sie den Kapazitätspool und die zugehörigen Volumes aus.
- c. Klicken Sie auf **Speichern**.
5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

## Erstellen von Sicherungsrichtlinien für SAP HANA-Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und eine Beschreibung ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie als Speichertyp \* Azure NetApp Files\* aus.
  - b. Wählen Sie **Dateibasiert**, wenn Sie eine Integritätsprüfung der Datenbank durchführen möchten.
  - c. Wählen Sie **Snapshot-basiert**, wenn Sie ein Backup mithilfe der Snapshot-Technologie erstellen möchten.
6. Führen Sie auf der Seite „Snapshot und Sicherung“ die folgenden Schritte aus:
  - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
  - b. Geben Sie die Aufbewahrungseinstellungen an.
  - c. Wenn Sie die Azure NetApp Files -Sicherung aktivieren möchten, wählen Sie **Sicherung aktivieren** und geben Sie die Aufbewahrungseinstellungen an.
7. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.

## Erstellen von Ressourcengruppen und Anfügen von SAP HANA-Sicherungsrichtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### 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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                          |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | Geben Sie einen Namen für die Ressourcengruppe ein.                                                                                              |
| Schlagwörter                                                  | Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten. |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
  - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
  - b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \*  \* für die Richtlinie, die Sie konfigurieren möchten.
  - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.
7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

## Sichern von SAP HANA-Datenbanken, die auf Azure NetApp Files ausgeführt werden

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:
  - a. Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen.



- b. Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.
- c. Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- d. Wählen Sie **Snapshot Copy Tool > SnapCenter ohne Dateisystemkonsistenz**, um Snapshots zu erstellen.

Die Option **Dateisystemkonsistenz** ist nur für Anwendungen anwendbar, die auf Windows-Hosts ausgeführt werden.

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

- a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
- b. Wählen \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamenname* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

9. Wählen Sie **Jetzt sichern**.

10. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, 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.

11. Wählen Sie **Backup**.

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

## Sichern von SAP HANA-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. 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 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. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Wiederherstellen und Wiederherstellen von SAP HANA-Datenbanken

Sie können Daten aus den Sicherungen wiederherstellen und wiederherstellen.

### Informationen zu diesem Vorgang

Wenn bei automatisch erkannten HANA-Systemen die Option **Vollständige Ressource** ausgewählt ist, erfolgt die Wiederherstellung mithilfe der Snapshot-Wiederherstellungstechnologie für einzelne Dateien. Wenn das Kontrollkästchen **Schnelle Wiederherstellung** aktiviert ist, wird die Volume Revert-Technologie verwendet.

Für manuell hinzugefügte Ressourcen wird immer die Volume Revert-Technologie verwendet.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.
3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf \*  \*.
6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option **Vollständige Ressource** aus.

Alle konfigurierten Datenvolumes der SAP HANA-Datenbank werden wiederhergestellt.

7. Führen Sie für automatisch erkannte HANA-Systeme auf der Seite „Wiederherstellungsbereich“ die folgenden Aktionen aus:
  - a. Wählen Sie **Auf den aktuellsten Stand wiederherstellen**, wenn Sie die Wiederherstellung so nah wie möglich an die aktuelle Zeit heranzuführen möchten.
  - b. Wählen Sie **Bis zu einem bestimmten Zeitpunkt wiederherstellen**, wenn Sie bis zum angegebenen Zeitpunkt wiederherstellen möchten.
  - c. Wählen Sie **Aus angegebener Datensicherung wiederherstellen**, wenn Sie eine Wiederherstellung aus einer bestimmten Datensicherung durchführen möchten.

- d. Wählen Sie **Keine Wiederherstellung**, wenn Sie jetzt keine Wiederherstellung wünschen.
- e. Geben Sie die Speicherorte für die Protokollsicherung an.
- f. Geben Sie den Speicherort des Sicherungskatalogs an.
8. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
9. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
10. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## Klonen Sie die SAP HANA-Datenbanksicherung

Sie können SnapCenter verwenden, um eine SAP HANA-Datenbank mithilfe der Sicherung der Datenbank zu klonen. Bei den erstellten Klonen handelt es sich um dicke Klone, die im übergeordneten Kapazitätspool erstellt werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.
3. Wählen Sie die Ressource oder Ressourcengruppe aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** vom primären Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:
  - a. Wählen Sie den Host aus, auf dem das SAP HANA-Plug-In zur Verwaltung des geklonten HANA-Systems installiert ist.

Es kann sich um einen zentralen Plug-In-Host oder einen HANA-Systemhost handeln.



Wenn das HANA-Plug-In auf einem zentralen Host installiert ist, der HANA-Datenbanken auf anderen Hosts verwaltet, überspringt SnapCenter beim Erstellen oder Löschen von Klonen absichtlich Host-seitige Vorgänge (Mounten oder Unmounten des Dateisystems), da der Zielsystem ein zentraler Host ist. Sie sollten benutzerdefinierte Skripte vor oder nach dem Klonen verwenden, um Mount- und Unmount-Vorgänge durchzuführen.

- a. Geben Sie die SAP HANA-SID ein, um aus den vorhandenen Sicherungen zu klonen.
- b. Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden.

- c. Wenn die ANF-Volumes der SAP HANA-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie das QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

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.
- b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Wenn das HANA-Quellsystem automatisch erkannt wird und das Plug-In für den Klonzielhost auf dem SAP HANA-Host installiert ist, trennt SnapCenter automatisch die Bereitstellung der vorhandenen HANA-Datenvolumes auf dem Klonzielhost und stellt die neu geklonten HANA-Datenvolumes bereit.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.



Clone Split ist für ANF-Klone deaktiviert, da der ANF-Klon bereits ein unabhängiges Volume ist, das aus dem ausgewählten Snapshot erstellt wurde.

## Schützen Sie Microsoft SQL Server-Datenbanken

### Hosts hinzufügen und SnapCenter Plug-In für SQL Server-Datenbank installieren

SnapCenter unterstützt den Datenschutz von SQL-Instanzen auf SMB-Freigaben auf Azure NetApp Files. Die eigenständigen und Verfügbarkeitsgruppenkonfigurationen (AG) werden unterstützt.

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen, und dann das Plug-In-Paket installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

#### Bevor Sie beginnen

- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.

#### Schritte

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

- a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
- b. Geben Sie im Feld „Hostname“ den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.
- c. Geben Sie im Feld „Anmeldeinformationen“ die von Ihnen erstellten Anmeldeinformationen ein.
5. Wählen Sie im Abschnitt **Zu installierende Plug-ins auswählen** die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Wählen Sie **Senden**.
8. Wählen Sie **Protokollverzeichnis konfigurieren**, geben Sie auf der Seite „Host-Protokollverzeichnis konfigurieren“ den SMB-Pfad des Host-Protokollverzeichnisses ein und klicken Sie auf **Speichern**.
9. Klicken Sie auf **Senden** und überwachen Sie den Installationsfortschritt.

## Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, bevor Sie SnapCenter zum Sichern von SQL Server-Ressourcen verwenden, oder Sie können eine Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine einzelne Ressource sichern.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und eine Beschreibung ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie als Speichertyp \* Azure NetApp Files\* aus.
  - b. Wählen Sie den Sicherungstyp aus.
    - i. Wählen Sie **Vollständige Sicherung und Protokollsicherung**, wenn Sie Datenbankdateien und Transaktionsprotokolle sichern möchten.
    - ii. Wählen Sie **Vollständige Sicherung**, wenn Sie nur die Datenbankdateien sichern möchten.
    - iii. Wählen Sie **Protokollsicherung**, wenn Sie nur die Transaktionsprotokolle sichern möchten.
    - iv. Wählen Sie **Nur Backup kopieren**, wenn Sie Ihre Ressourcen mithilfe einer anderen Anwendung sichern möchten.
  - c. Führen Sie im Abschnitt „Einstellungen der Verfügbarkeitsgruppe“ die folgenden Aktionen aus:
    - i. Wählen Sie „Auf bevorzugter Sicherungsreplik sichern“, wenn Sie nur auf der Replik sichern möchten.
    - ii. Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für die Sicherung aus.
    - iii. Wählen Sie die Sicherungspriorität aus.
6. Führen Sie auf der Seite „Snapshot und Sicherung“ die folgenden Schritte aus:
  - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
  - b. Geben Sie die Aufbewahrungseinstellungen je nach ausgewähltem Sicherungstyp an.
  - c. Wenn Sie die Azure NetApp Files -Sicherung aktivieren möchten, wählen Sie **Sicherung aktivieren**

und geben Sie die Aufbewahrungseinstellungen an.

7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

- a. Wählen Sie im Abschnitt „Überprüfung für folgende Sicherungszeitpläne ausführen“ die Zeitplanhäufigkeit aus.
- b. Führen Sie im Abschnitt „Optionen zur Datenbankkonsistenzprüfung“ die folgenden Aktionen aus:
  - i. Wählen Sie **Integritätsstruktur auf die physische Struktur der Datenbank beschränken (NUR\_PHYSIKALISCH)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu beschränken und zerrissene Seiten, Prüfsummenfehler und allgemeine Hardwarefehler zu erkennen, die sich auf die Datenbank auswirken.
  - ii. Wählen Sie **Alle Informationsmeldungen unterdrücken (NO\_INFOMSGS)**, um alle Informationsmeldungen zu unterdrücken.

Standardmäßig ausgewählt.

- iii. Wählen Sie **Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL\_ERRORMSGs)**, um alle gemeldeten Fehler pro Objekt anzuzeigen.
- iv. Wählen Sie **Nicht gruppierte Indizes nicht prüfen (NOINDEX)** aus, wenn Sie keine nicht gruppierten Indizes prüfen möchten.

Die SQL Server-Datenbank verwendet den Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.

- v. Wählen Sie **Beschränken Sie die Prüfungen und erhalten Sie die Sperren, anstatt eine interne Datenbank-Snapshot-Kopie zu verwenden (TABLOCK)** aus, um die Prüfungen zu begrenzen und Sperren zu erhalten, anstatt einen internen Datenbank-Snapshot zu verwenden.
- c. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss überprüfen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
- d. Geben Sie im Abschnitt **Einstellungen des Überprüfungsskripts** den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Überprüfungsvorgang ausgeführt werden soll.

8. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.

## Erstellen von Ressourcengruppen und Anfügen von SQL-Sicherungsrichtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### 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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                          |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | Geben Sie einen Namen für die Ressourcengruppe ein.                                                                                              |
| Schlagwörter                                                  | Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten. |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
  - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
  - b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \*  \* für die Richtlinie, die Sie konfigurieren möchten.
  - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.
  - d. Wählen Sie den Microsoft SQL Server-Scheduler aus.
7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
  - a. Wählen Sie den Verifizierungsserver aus.
  - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf \*  \*.
  - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
  - d. Klicken Sie auf **OK**.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

## Sichern von SQL Server-Datenbanken, die auf Azure NetApp Files ausgeführt werden

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Bevor Sie beginnen

Sie sollten einen Lastenausgleich erstellen, wenn dem Azure Windows-Failovercluster keine Cluster-IP zugewiesen ist oder er von SnapCenter aus nicht erreichbar ist. Die IP des Load Balancers sollte konfiguriert

und vom SnapCenter -Server aus erreichbar sein.

## Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Ressourcenseite aus der Dropdownliste „Anzeigen“ die Option „Datenbank“, „Instanz“ oder „Verfügbarkeitsgruppe“ aus.
3. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
4. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
  - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
  - b. Wählen \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
  - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

*policy\_name* ist der Name der von Ihnen ausgewählten Richtlinie.

- d. Wählen Sie **Microsoft SQL Server-Scheduler verwenden** und wählen Sie dann aus der Dropdown-Liste **Scheduler-Instanz** die Scheduler-Instanz aus, die der Planungsrichtlinie zugeordnet ist.
5. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
    - a. Wählen Sie den Verifizierungsserver aus.
    - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf \*  \*.
    - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
    - d. Klicken Sie auf OK.
  6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
  7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
  8. Wählen Sie **Jetzt sichern**.
  9. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
    - a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
    - b. Wählen Sie **Nach Sicherung überprüfen**.
    - c. Wählen Sie **Backup**.
  10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

## Sichern von SQL Server-Ressourcengruppen

Sie können Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe



definierten Ressourcen ausgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. 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 Richtlinie aus, die Sie für die Sicherung verwenden möchten.
  - b. Wählen Sie nach der Sicherung „Überprüfen“ aus, um die On-Demand-Sicherung zu überprüfen.
  - c. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Wiederherstellen und Wiederherstellen von SQL Server-Datenbanken

Sie können SnapCenter verwenden, um gesicherte SQL Server-Datenbanken wiederherzustellen. Die Datenbankwiederherstellung ist ein mehrphasiger Prozess, bei dem alle Daten und Protokollseiten aus einer angegebenen SQL Server-Sicherung in eine angegebene Datenbank kopiert werden.

### Informationen zu diesem Vorgang

Sie sollten sicherstellen, dass die Zielinanz für die Wiederherstellung mit einem Active Directory-Benutzer konfiguriert ist, der zur Active Directory-Domäne SMB AD gehört und über die Berechtigung verfügt, die Dateiberechtigungen entsprechend festzulegen. Sie sollten die Anmeldeinformationen in SnapCenter auf Instanzebene konfigurieren.

Die SQL-Authentifizierung für die Zielinanz wird für SMB-Konfigurationen nicht unterstützt. Die Zielinanz sollte in SnapCenter mit dem Active Directory-Benutzer konfiguriert werden, der über die erforderlichen Berechtigungen verfügt.

Wenn das Dienstkonto der SnapCenter Plug-in-Dienste kein Active Directory-Benutzer ist, wird beim Durchführen der Wiederherstellung auf einem alternativen Host der Benutzer benötigt, der die vollständige Kontrolle über die Quellvolumes hat, damit dieser seine Identität annehmen und den erforderlichen Vorgang ausführen kann.

### 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“ entweder „**Datenbank**“ oder „**Ressourcengruppe**“ aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option „**Backups** vom Speichersystem“ aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf das  Symbol.
6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:

- a. Wählen Sie **Datenbank auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde**, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Sicherungen erstellt wurden.
  - b. Wählen Sie **Datenbank auf einem anderen Host wiederherstellen**, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem die Sicherungen erstellt werden.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
- a. Wählen Sie **Keine**, wenn Sie nur die vollständige Sicherung ohne Protokolle wiederherstellen müssen.
  - b. Wählen Sie den minutengenauen Wiederherstellungsvorgang „Alle Protokollsicherungen“ aus, um alle verfügbaren Protokollsicherungen nach der vollständigen Sicherung wiederherzustellen.
  - c. Wählen Sie **Nach Protokollsicherungen** aus, um einen Wiederherstellungsvorgang zu einem bestimmten Zeitpunkt durchzuführen, bei dem die Datenbank basierend auf Sicherungsprotokollen bis zum Sicherungsprotokoll mit dem ausgewählten Datum wiederhergestellt wird.
  - d. Wählen Sie **Bis zu einem bestimmten Datum bis** aus, um das Datum und die Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht mehr auf die wiederhergestellte Datenbank angewendet werden.
  - e. Wenn Sie **Alle Protokollsicherungen**, **Nach Protokollsicherungen** oder **Nach bestimmtem Datum bis** ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie **Benutzerdefiniertes Protokollverzeichnis verwenden** und geben Sie dann den Protokollspeicherort an.
8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

## Klonen Sie die SQL Server-Datenbanksicherung

Sie können SnapCenter verwenden, um eine SQL-Datenbank mithilfe der Sicherung der Datenbank zu klonen. Bei den erstellten Klonen handelt es sich um dicke Klone, die im übergeordneten Kapazitätspool erstellt werden.

### Informationen zu diesem Vorgang

Sie sollten sicherstellen, dass die Zielinstanz für den Klon mit einem Active Directory-Benutzer konfiguriert ist, der zur Active Directory-Domäne SMB AD gehört und über die Berechtigung verfügt, die Dateiberechtigungen entsprechend festzulegen. Sie sollten die Anmeldeinformationen in SnapCenter auf Instanzebene konfigurieren.

Die SQL-Authentifizierung für die Zielinstanz wird für SMB-Konfigurationen nicht unterstützt. Die Zielinstanz sollte in SnapCenter mit dem Active Directory-Benutzer konfiguriert werden, der über die erforderlichen Berechtigungen verfügt.

Wenn das Dienstkonto der SnapCenter Plug-in-Dienste kein Active Directory-Benutzer ist, wird beim Klonen der Benutzer benötigt, der die vollständige Kontrolle über die Quellvolumes hat, damit seine Identität angenommen werden kann und der erforderliche Vorgang ausgeführt werden kann.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In

aus der Liste aus.

2. Wählen Sie auf der Seite „Ressourcen“ entweder „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** die Sicherung vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus und wählen Sie dann \*  \*.
6. Geben Sie auf der Seite **Klonoptionen** alle erforderlichen Details ein.
7. Wählen Sie auf der Seite „Speicherort“ einen Speicherort aus, um einen Klon zu erstellen.

Wenn die ANF-Volumes der SQL Server-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie die QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Wählen Sie auf der Seite „Protokolle“ eine der folgenden Optionen aus:
  - a. Wählen Sie **Keine**, wenn Sie nur die vollständige Sicherung ohne Protokolle klonen möchten.
  - b. Wählen Sie **Alle Protokollsicherungen** aus, wenn Sie alle verfügbaren Protokollsicherungen mit Datum nach der vollständigen Sicherung klonen möchten.
  - c. Wählen Sie **Nach Protokollsicherungen bis**, wenn Sie die Datenbank basierend auf den Sicherungsprotokollen klonen möchten, die bis zum Sicherungsprotokoll mit dem ausgewählten Datum erstellt wurden.
  - d. Wählen Sie **Nach bestimmtem Datum bis** aus, wenn Sie die Transaktionsprotokolle nach dem angegebenen Datum und der angegebenen Uhrzeit nicht mehr anwenden möchten.
9. Geben Sie auf der Seite **Skript** das Skript-Timeout, den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Klonvorgang ausgeführt werden soll.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
11. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Klon-Lebenszyklus durchführen

Mit SnapCenter können Sie Klone aus einer Ressourcengruppe oder Datenbank erstellen. Sie können entweder einen On-Demand-Klon durchführen oder wiederkehrende Klonvorgänge einer Ressourcengruppe oder Datenbank planen. Wenn Sie regelmäßig ein Backup klonen, können Sie den Klon zum Entwickeln von Anwendungen, Auffüllen von Daten oder Wiederherstellen von Daten verwenden.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** die Sicherung vom primären Speichersystem aus.

5. Wählen Sie die Sicherung aus und wählen Sie dann \*  \*.
6. Geben Sie auf der Seite **Klonooptionen** alle erforderlichen Details ein.
7. Wählen Sie auf der Seite „Speicherort“ einen Speicherort aus, um einen Klon zu erstellen.

Wenn die ANF-Volumes der SQL Server-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie die QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Geben Sie auf der Seite **Skript** das Skript-Timeout, den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Klonvorgang ausgeführt werden soll.
9. Führen Sie auf der Seite „Planen“ eine der folgenden Aktionen aus:
  - Wählen Sie **Jetzt ausführen**, wenn Sie den Klonauftrag sofort ausführen möchten.
  - Wählen Sie **Zeitplan konfigurieren** aus, wenn Sie festlegen möchten, wie häufig der Klonvorgang erfolgen soll, wann der Klonzeitplan beginnen soll, an welchem Tag der Klonvorgang erfolgen soll, wann der Zeitplan ablaufen soll und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
11. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Schützen Sie Oracle-Datenbanken

### Hosts hinzufügen und SnapCenter Plug-In für Oracle-Datenbank installieren

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

Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie das Plug-in auf einem Cluster (Oracle RAC) installieren, wird das Plug-in auf allen Knoten des Clusters installiert. Für Oracle RAC One Node sollten Sie das Plug-in sowohl auf aktiven als auch auf passiven Knoten installieren.

#### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:
  - a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
  - b. Geben Sie im Feld „Hostname“ den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.
  - c. Geben Sie im Feld „Anmeldeinformationen“ die von Ihnen erstellten Anmeldeinformationen ein.
5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Klicken Sie auf **Senden**.
8. Überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.

9. Überwachen Sie den Installationsfortschritt.

## Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken

Bevor Sie SnapCenter zum Sichern von Oracle-Datenbankressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, die Sie sichern möchten.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie „Oracle-Datenbank“ aus der Dropdownliste aus.
4. Klicken Sie auf **Neu**.
5. Geben Sie auf der Seite „Name“ den Richtliniennamen und eine Beschreibung ein.
6. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
  - a. Wählen Sie als Speichertyp \* Azure NetApp Files\* aus.
  - b. Wählen Sie als Sicherungstyp entweder Online- oder Offline-Sicherung aus.
  - c. Wenn Sie die Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren**.
  - d. Wenn Sie Archivprotokolle nach der Sicherung bereinigen möchten, wählen Sie **Archivprotokolle nach der Sicherung bereinigen**.
  - e. Geben Sie die Einstellungen zum Löschen des Archivprotokolls an.
7. Führen Sie auf der Seite „Snapshot und Sicherung“ die folgenden Schritte aus:
  - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
  - b. Geben Sie die Aufbewahrungseinstellungen an.
  - c. Wenn Sie die Azure NetApp Files -Sicherung aktivieren möchten, wählen Sie **Sicherung aktivieren** und geben Sie die Aufbewahrungseinstellungen an.
8. 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.
9. Wählen Sie auf der Seite „Überprüfung“ den Sicherungszeitplan aus, für den Sie den Überprüfungsvorgang durchführen möchten, und geben Sie den Pfad und die Argumente des Präskripts oder Postskripts ein, das Sie vor bzw. nach dem Überprüfungsvorgang ausführen möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.

## Erstellen Sie Ressourcengruppen und fügen Sie Oracle-Sicherungsrichtlinien hinzu

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen,

die Sie sichern und schützen möchten.

Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

### 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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

| Für dieses Feld...                                            | Machen Sie Folgendes...                                                                                                                          |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                          | Geben Sie einen Namen für die Ressourcengruppe ein.                                                                                              |
| Schlagwörter                                                  | Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.                                  |
| Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden | Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten. |
| Ziel der Archivprotokolldatei                                 | Geben Sie die Ziele der Archivprotokolldateien an.                                                                                               |

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
  - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
  - b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf \*  \* für die Richtlinie, die Sie konfigurieren möchten.
  - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.
7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
  - a. Wählen Sie den Verifizierungsserver aus.
  - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf \*  .
  - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
  - d. Klicken Sie auf **OK**.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

## Sichern von Oracle-Datenbanken, die auf Azure NetApp Files ausgeführt werden

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Ressourcenseite in der Dropdownliste „Ansicht“ die Option „Datenbank“ aus.
3. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
4. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
  - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
  - b. Wählen \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
  - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.
5. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
  - a. Wählen Sie den Verifizierungsserver aus.
  - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf \*  \*.
  - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
  - d. Klicken Sie auf OK.
6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
  - a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
  - b. Klicken Sie auf **Sichern**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

## Sichern von Oracle-Ressourcengruppen

Sie können Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Ein

Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

#### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. 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 Richtlinie aus, die Sie für die Sicherung verwenden möchten.
  - b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

## Wiederherstellen und Wiederherstellen von Oracle-Datenbanken

Im Falle eines Datenverlusts können Sie mit SnapCenter Daten aus einem oder mehreren Backups auf Ihrem aktiven Dateisystem wiederherstellen und anschließend die Datenbank wiederherstellen.

#### 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“ entweder **Datenbank** oder **Ressourcengruppe** aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** vom primären Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf \*  \*.
6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
  - a. Wählen Sie RAC, wenn Sie eine Sicherung einer Datenbank in einer RAC-Umgebung ausgewählt haben.
  - b. Führen Sie die folgenden Aktionen aus:
    - i. Wählen Sie **Alle Datendateien**, wenn Sie nur die Datenbankdateien wiederherstellen möchten.
    - ii. Wählen Sie **Tablespaces**, wenn Sie nur die Tablespaces wiederherstellen möchten.
    - iii. Wählen Sie **Redo-Log-Dateien**, wenn Sie die Redo-Log-Dateien der Data Guard-Standby- oder Active Data Guard-Standby-Datenbanken wiederherstellen möchten.
    - iv. Wählen Sie **Pluggable Databases** und geben Sie die PDBs an, die Sie wiederherstellen möchten.
    - v. Wählen Sie **Pluggable Database (PDB)-Tablespaces** aus und geben Sie dann die PDB und die Tablespaces dieser PDB an, die Sie wiederherstellen möchten.
    - vi. Wählen Sie **Datenbank auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde**, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Sicherungen erstellt wurden.



- vii. Wählen Sie **Datenbank auf einem anderen Host wiederherstellen**, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem die Sicherungen erstellt werden.
  - viii. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.
  - ix. Wählen Sie **In-Place-Wiederherstellung erzwingen**, wenn Sie eine In-Place-Wiederherstellung in Szenarien durchführen möchten, in denen nach der Sicherung neue Datendateien hinzugefügt werden oder wenn LUNs zu einer LVM-Datenträgergruppe hinzugefügt, gelöscht oder neu erstellt werden.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
    - a. Wählen Sie **Alle Protokolle**, wenn Sie die letzte Transaktion wiederherstellen möchten.
    - b. Wählen Sie **Bis SCN (System Change Number)**, wenn Sie zu einer bestimmten SCN wiederherstellen möchten.
    - c. Wählen Sie **Datum und Uhrzeit**, wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten.
    - d. Wählen Sie **Keine Wiederherstellung**, wenn Sie keine Wiederherstellung wünschen.
    - e. Wählen Sie **Externe Archivprotokollspeicherorte angeben**, wenn Sie den Speicherort der externen Archivprotokolldateien angeben möchten.
  8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
  9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
  10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
  11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

## Wiederherstellen und Wiederherstellen von Tablespaces mithilfe der Point-in-Time-Wiederherstellung

Sie können eine Teilmenge beschädigter oder gelöschter Tablespaces wiederherstellen, ohne dass dies Auswirkungen auf die anderen Tablespaces in der Datenbank hat. SnapCenter verwendet RMAN, um eine Point-in-Time-Wiederherstellung (PITR) der Tablespaces durchzuführen.

### 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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (Multitenant)“ aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus dem Speichersystem aus.

Wenn das Backup nicht katalogisiert ist, sollten Sie das Backup auswählen und auf **Katalog** klicken.

5. Wählen Sie das katalogisierte Backup aus und klicken Sie dann auf \*  \*.
6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
  - a. Wählen Sie **RAC**, wenn Sie eine Sicherung einer Datenbank in einer RAC-Umgebung ausgewählt haben.

- b. Wählen Sie **Tablespaces**, wenn Sie nur die Tablespaces wiederherstellen möchten.
  - c. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
    - a. Wählen Sie **Bis SCN (System Change Number)**, wenn Sie zu einer bestimmten SCN wiederherstellen möchten.
    - b. Wählen Sie **Datum und Uhrzeit**, wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten.
  8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
  9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
  10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
  11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

## Wiederherstellen und Wiederherstellen einer steckbaren Datenbank mithilfe der Point-in-Time-Wiederherstellung

Sie können eine Pluggable Database (PDB), die beschädigt oder gelöscht wurde, wiederherstellen, ohne dass dies Auswirkungen auf die anderen PDBs in der Containerdatenbank (CDB) hat. SnapCenter verwendet RMAN, um eine Point-in-Time-Wiederherstellung (PITR) der PDB durchzuführen.

### 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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (Multitenant)“ aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus dem Speichersystem aus.

Wenn das Backup nicht katalogisiert ist, sollten Sie das Backup auswählen und auf **Katalog** klicken.

5. Wählen Sie das katalogisierte Backup aus und klicken Sie dann auf \*  \*.
6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
  - a. Wählen Sie **RAC**, wenn Sie eine Sicherung einer Datenbank in einer RAC-Umgebung ausgewählt haben.
  - b. Führen Sie eine der folgenden Aktionen aus, je nachdem, ob Sie die PDB oder Tablespaces in einer PDB wiederherstellen möchten:
    - Wählen Sie **Pluggable Databases (PDBs)**, wenn Sie eine PDB wiederherstellen möchten.
    - Wählen Sie **Pluggable Database (PDB)-Tablespaces** aus, wenn Sie Tablespaces in einer PDB wiederherstellen möchten.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
  - a. Wählen Sie **Bis SCN (System Change Number)**, wenn Sie zu einer bestimmten SCN wiederherstellen möchten.

- b. Wählen Sie **Datum und Uhrzeit**, wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten.
8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

## Klonen Sie die Oracle-Datenbanksicherung

Sie können SnapCenter verwenden, um eine Oracle-Datenbank mithilfe der Sicherung der Datenbank zu klonen. Bei den erstellten Klonen handelt es sich um dicke Klone, die im übergeordneten Kapazitätspool erstellt werden.

### 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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank aus.
4. Wählen Sie auf der Ansichtsseite „Kopien verwalten“ die Sicherung vom primären Speichersystem aus.
5. Wählen Sie die Datensicherung aus und klicken Sie dann auf \*  \*.
6. Wählen Sie auf der Seite „Name“ aus, ob Sie eine Datenbank (CDB oder nicht CDB) oder eine Pluggable-Datenbank (PDB) klonen möchten.
7. Geben Sie auf der Seite „Standorte“ die erforderlichen Details an.

Wenn die ANF-Volumes der Oracle-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie das QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Führen Sie auf der Seite „Anmeldeinformationen“ einen der folgenden Schritte aus:
  - a. Wählen Sie unter Anmeldeinformationsname für Sys-Benutzer die Anmeldeinformationen aus, die zum Definieren des Sys-Benutzerkennworts der Klondatenbank verwendet werden sollen.
  - b. Wählen Sie für den Anmeldeinformationsnamen der ASM-Instanz **Keine** aus, wenn die Betriebssystemauthentifizierung für die Verbindung mit der ASM-Instanz auf dem Klonhost aktiviert ist.

Andernfalls wählen Sie die Oracle ASM-Anmeldeinformationen aus, die entweder mit dem Benutzer „sys“ oder einem Benutzer mit der für den Klonhost geltenden Berechtigung „sysasm“ konfiguriert sind.

9. Geben Sie auf der Seite „Pre-Ops“ den Pfad und die Argumente der Prescripts an und ändern Sie im Abschnitt „Datenbankparametereinstellungen“ die Werte der vorab ausgefüllten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
10. Auf der Seite „Post-Ops“ sind standardmäßig **„Datenbank wiederherstellen“** und **„Bis Abbrechen“** ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

- a. Wenn Sie „Bis Abbrechen“ auswählen, führt SnapCenter die Wiederherstellung durch, indem es die neueste Protokollsicherung mit der ununterbrochenen Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung bereitstellt.
- b. Wenn Sie **Datum und Uhrzeit** auswählen, stellt SnapCenter die Datenbank bis zu einem angegebenen Datum und einer angegebenen Uhrzeit wieder her.
- c. Wenn Sie **Bis SCN** auswählen, stellt SnapCenter die Datenbank bis zu einem angegebenen SCN wieder her.
- d. Wenn Sie **Externe Archivprotokollspeicherorte angeben** auswählen, ermittelt und mountet SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit.
- e. Standardmäßig ist das Kontrollkästchen **Neue DBID erstellen** aktiviert, um eine eindeutige Nummer (DBID) für die geklonte Datenbank zu generieren, die sie von der Quelldatenbank unterscheidet.

Deaktivieren Sie das Kontrollkästchen, wenn Sie der geklonten Datenbank die DBID der Quelldatenbank zuweisen möchten. Wenn Sie in diesem Szenario die geklonte Datenbank beim externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.

- f. Aktivieren Sie das Kontrollkästchen **Temporäre Datei für temporären Tablespace erstellen**, wenn Sie eine temporäre Datei für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten.
  - g. Fügen Sie unter **Geben Sie SQL-Einträge ein, die beim Erstellen des Klons angewendet werden sollen** die SQL-Einträge hinzu, die beim Erstellen des Klons angewendet werden sollen.
  - h. Geben Sie unter **Geben Sie die nach dem Klonvorgang auszuführenden Skripts ein** den Pfad und die Argumente des Postskripts an, das Sie nach dem Klonvorgang ausführen möchten.
11. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
  12. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
  13. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen > Jobs** auswählen.

## Klonen einer steckbaren Datenbank

Sie können eine Pluggable Database (PDB) auf eine andere oder dieselbe Ziel-CDB auf demselben Host oder einem alternativen Host klonen. Sie können die geklonte PDB auch zu einem gewünschten SCN oder Datum und einer gewünschten Uhrzeit wiederherstellen.

### 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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstantz (Multitenant)“ aus.
4. Wählen Sie auf der Ansichtsseite „Kopien verwalten“ die Sicherung vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus und klicken Sie dann auf \*  \*.
6. Wählen Sie auf der Seite „Name“ **PDB-Klon** aus und geben Sie die anderen Details an.
7. Geben Sie auf der Seite „Standorte“ die erforderlichen Details an.

8. Geben Sie auf der Seite „Pre-Ops“ den Pfad und die Argumente der Prescripts an und ändern Sie im Abschnitt „Datenbankparametereinstellungen“ die Werte der vorab ausgefüllten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
9. Auf der Seite „Post-Ops“ ist standardmäßig **„Bis Abbrechen“** ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.
  - a. Wenn Sie „Bis Abbrechen“ auswählen, führt SnapCenter die Wiederherstellung durch, indem es die neueste Protokollsicherung mit der ununterbrochenen Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung bereitstellt.
  - b. Wenn Sie **Datum und Uhrzeit** auswählen, stellt SnapCenter die Datenbank bis zu einem angegebenen Datum und einer angegebenen Uhrzeit wieder her.
  - c. Wenn Sie **Externe Archivprotokollspeicherorte angeben** auswählen, ermittelt und mountet SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit.
  - d. Standardmäßig ist das Kontrollkästchen **Neue DBID erstellen** aktiviert, um eine eindeutige Nummer (DBID) für die geklonte Datenbank zu generieren, die sie von der Quelldatenbank unterscheidet.  
  
 Deaktivieren Sie das Kontrollkästchen, wenn Sie der geklonten Datenbank die DBID der Quelldatenbank zuweisen möchten. Wenn Sie in diesem Szenario die geklonte Datenbank beim externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.
  - e. Aktivieren Sie das Kontrollkästchen **Temporäre Datei für temporären Tablespace erstellen**, wenn Sie eine temporäre Datei für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten.
  - f. Fügen Sie unter **Geben Sie SQL-Einträge ein, die beim Erstellen des Klons angewendet werden sollen** die SQL-Einträge hinzu, die beim Erstellen des Klons angewendet werden sollen.
  - g. Geben Sie unter **Geben Sie die nach dem Klonvorgang auszuführenden Skripts ein** den Pfad und die Argumente des Postskripts an, das Sie nach dem Klonvorgang ausführen möchten.
10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
11. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen > Jobs** auswählen.

# Verwalten von SnapCenter Server und Plug-Ins

## Dashboard anzeigen

### Übersicht über das Dashboard

Über das Dashboard im linken Navigationsbereich von SnapCenter erhalten Sie einen ersten Überblick über den Zustand Ihres Systems, einschließlich der letzten Jobaktivität, Warnungen, Schutzzusammenfassung, Speichereffizienz und -nutzung, Status von SnapCenter -Jobs (Sichern, Klonen, Wiederherstellen), Konfigurationsstatus für eigenständige und Windows-Cluster-Hosts, Anzahl der von SnapCenter verwalteten Storage Virtual Machines (SVMs) und Lizenzkapazität.

Die in der Dashboard-Ansicht angezeigten Informationen hängen von der Rolle ab, die dem Benutzer zugewiesen ist, der derzeit bei SnapCenter angemeldet ist. Einige Inhalte werden möglicherweise nicht angezeigt, wenn der Benutzer nicht über die Berechtigung zum Anzeigen dieser Informationen verfügt.

In vielen Fällen können Sie weitere Informationen zu einer Anzeige anzeigen, indem Sie mit der Maus über i fahren. In einigen Fällen sind Informationen in Dashboard-Anzeigen mit detaillierten Quellinformationen auf SnapCenter GUI-Seiten wie Ressourcen, Monitor und Berichten verknüpft.

### Aktuelle Arbeitsaktivitäten

Die Kachel „Letzte Jobaktivitäten“ zeigt die neuesten Jobaktivitäten aller Sicherungs-, Wiederherstellungs- und Klonjobs an, auf die Sie Zugriff haben. Jobs in dieser Anzeige haben einen der folgenden Status: Abgeschlossen, Warnung, Fehlgeschlagen, Wird ausgeführt, In der Warteschlange und Abgebrochen.

Wenn Sie mit der Maus über einen Job fahren, werden weitere Informationen angezeigt. Sie können zusätzliche Auftragsinformationen anzeigen, indem Sie auf eine bestimmte Auftragsnummer klicken. Dadurch werden Sie zur Monitorseite weitergeleitet. Von dort aus können Sie Auftragsdetails oder Protokollinformationen abrufen und einen spezifischen Bericht für diesen Auftrag erstellen.

Klicken Sie auf **Alle anzeigen**, um einen Verlauf aller SnapCenter -Jobs anzuzeigen.

### Warnungen

Die Kachel „Warnungen“ zeigt die neuesten ungelösten kritischen und Warnmeldungen für die Hosts und den SnapCenter -Server an.

Die Gesamtzahl der Warnungen der Kategorien „Kritisch“ und „Warnung“ wird oben im Display angezeigt. Wenn Sie auf die Gesamtsummen „Kritisch“ oder „Warnung“ klicken, werden Sie auf die Seite „Warnungen“ weitergeleitet, auf der der jeweilige Filter angewendet wird.

Wenn Sie auf eine bestimmte Warnung klicken, werden Sie auf die Seite „Warnungen“ weitergeleitet, auf der Sie Einzelheiten zu dieser Warnung finden. Wenn Sie unten in der Anzeige auf **Alle anzeigen** klicken, werden Sie auf die Seite „Warnungen“ weitergeleitet, wo Sie eine Liste aller Warnungen sehen.

### Neueste Schutzzusammenfassung

Die Kachel „Neueste Schutzzusammenfassung“ zeigt Ihnen den Schutzstatus für alle Entitäten an, auf die Sie Zugriff haben. Standardmäßig ist die Anzeige so eingestellt, dass der Status aller Plug-Ins angezeigt wird. Statusinformationen werden für Ressourcen bereitgestellt, die als Snapshots auf dem Primärspeicher und

mithilfe der Technologien SnapMirror und SnapVault auf dem Sekundärspeicher gesichert werden. Die Verfügbarkeit von Schutzstatusinformationen für den Sekundärspeicher hängt vom ausgewählten Plug-In-Typ ab.



Wenn Sie eine Mirror-Vault-Schutzrichtlinie verwenden, werden die Zähler für die Schutzzusammenfassung im SnapVault Zusammenfassungsdiagramm und nicht im SnapMirror Diagramm angezeigt.

Der Schutzstatus für einzelne Plug-Ins ist verfügbar, indem Sie ein Plug-In aus dem Dropdown-Menü auswählen. Ein Ringdiagramm zeigt den Prozentsatz der geschützten Ressourcen für das ausgewählte Plug-in. Durch Klicken auf ein Ringdiagramm gelangen Sie zur Seite **Berichte > Plug-in**, die einen detaillierten Bericht aller primären und sekundären Speicheraktivitäten für das angegebene Plug-in enthält.



Berichte zum Sekundärspeicher gelten nur für SnapVault ; SnapMirror -Berichte werden nicht unterstützt.



SAP HANA bietet Informationen zum Schutzstatus für den primären und sekundären Speicher für Snapshots. Für dateibasierte Sicherungen ist nur der Schutzstatus des primären Speichers verfügbar.

| Schutzstatus       | Primärspeicher                                                                                                                                                 | Sekundärspeicher                                                                                                                                                   |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fehlgeschlagen     | Anzahl der Entitäten, die Teil einer Ressourcengruppe sind, wobei die Ressourcengruppe eine Sicherung ausgeführt hat, die Sicherung jedoch fehlgeschlagen ist. | Anzahl der Entitäten mit Sicherungen, deren Übertragung an ein sekundäres Ziel fehlgeschlagen ist.                                                                 |
| Erfolgreich        | Anzahl der Entitäten in einer Ressourcengruppe, wobei die Ressourcengruppe erfolgreich gesichert wurde.                                                        | Anzahl der Entitäten mit Sicherungen, die erfolgreich an ein sekundäres Ziel übertragen wurden.                                                                    |
| Nicht konfiguriert | Anzahl der Entitäten, die nicht Teil einer Ressourcengruppe sind und nicht gesichert wurden.                                                                   | Anzahl der Entitäten, die Teil einer oder mehrerer Ressourcengruppen sind, die nicht für die Übertragung von Sicherungen an ein sekundäres Ziel konfiguriert sind. |
| Nicht initiiert    | Anzahl der Entitäten, die Teil einer Ressourcengruppe sind, für die aber keine Sicherung ausgeführt wurde.                                                     | Nicht zutreffend.                                                                                                                                                  |



Wenn Sie SnapCenter Server 4.2 und eine frühere Version des Plug-Ins (älter als 4.2) zum Erstellen von Sicherungen verwenden, wird auf der Kachel „Neueste Schutzzusammenfassung“ der SnapMirror Schutzstatus dieser Sicherungen nicht angezeigt.

## Jobs

Die Kachel „Jobs“ bietet Ihnen eine Zusammenfassung der Sicherungs-, Wiederherstellungs- und Klonjobs, auf die Sie Zugriff haben. Sie können den Zeitrahmen für jeden Bericht mithilfe des Dropdown-Menüs anpassen. Die Zeitrahmenoptionen sind auf die letzten 24 Stunden, die letzten 7 Tage und die letzten 30 Tage festgelegt. Der Standardbericht zeigt die Datenschutzjobs, die in den letzten 7 Tagen ausgeführt wurden.

Informationen zu Sicherungs-, Wiederherstellungs- und Klonaufträgen werden in Ringdiagrammen angezeigt. Wenn Sie auf ein Donut-Segment klicken, werden Sie zur Monitorseite weitergeleitet, auf deren Auswahl bereits Jobfilter angewendet sind.

| Auftragsstatus  | Beschreibung                                           |
|-----------------|--------------------------------------------------------|
| Fehlgeschlagen  | Anzahl der fehlgeschlagenen Jobs.                      |
| Warnung         | Anzahl der Jobs, bei denen ein Fehler aufgetreten ist. |
| Erfolgreich     | Anzahl der erfolgreich abgeschlossenen Jobs.           |
| Wird ausgeführt | Anzahl der Jobs, die derzeit ausgeführt werden.        |

## Storage

Die Kachel „Speicher“ zeigt den von Schutzaufträgen über einen Zeitraum von 90 Tagen verbrauchten Primär- und Sekundärspeicher an, stellt Verbrauchstrends grafisch dar und berechnet die Einsparungen beim Primärspeicher. Die Speicherinformationen werden alle 24 Stunden um 0 Uhr aktualisiert.

Der Gesamtverbrauch des Tages, der sich aus der Gesamtzahl der in SnapCenter verfügbaren Backups und der von diesen Backups belegten Größe zusammensetzt, wird oben auf dem Display angezeigt. Einem Backup können mehrere Snapshots zugeordnet sein und die Anzahl spiegelt dies wider. Dies gilt sowohl für primäre als auch für sekundäre Snapshots. Beispiel: Sie haben 10 Sicherungen erstellt, von denen 2 aufgrund der richtlinienbasierten Sicherungsaufbewahrung gelöscht werden und 1 Sicherung ausdrücklich von Ihnen gelöscht wird. Daher wird die Anzahl von 7 Sicherungen zusammen mit der von diesen 7 Sicherungen belegten Größe angezeigt.

Der Speichereinsparungsfaktor für den Primärspeicher ist das Verhältnis der logischen Kapazität (Einsparungen durch Klone und Snapshots plus verbrauchter Speicher) zur physischen Kapazität des Primärspeichers. Ein Balkendiagramm veranschaulicht die Speichereinsparungen.

Das Liniendiagramm stellt den Primär- und Sekundärspeicherverbrauch über einen rollierenden 90-Tage-Zeitraum hinweg getrennt auf Tagesbasis dar. Wenn Sie mit der Maus über die Diagramme fahren, werden detaillierte Tagesergebnisse angezeigt.



Wenn Sie SnapCenter Server 4.2 und eine frühere Version des Plug-Ins (älter als 4.2) zum Erstellen von Sicherungen verwenden, werden auf der Kachel „Speicher“ weder die Anzahl der Sicherungen, der von diesen Sicherungen belegte Speicher noch die Snapshot-Einsparungen, die Klon-Einsparungen und die Snapshot-Größe angezeigt.

## Konfiguration

Die Kachel „Konfiguration“ bietet konsolidierte Statusinformationen für alle aktiven eigenständigen und Windows-Cluster-Hosts, die von SnapCenter verwaltet werden und auf die Sie Zugriff haben. Dazu gehören



die mit diesen Hosts verknüpften Plug-In-Statusinformationen.

Wenn Sie auf die Zahl neben „Hosts“ klicken, werden Sie zum Abschnitt „Verwaltete Hosts“ auf der Seite „Hosts“ weitergeleitet. Von dort aus können Sie detaillierte Informationen zu einem ausgewählten Host erhalten.

Darüber hinaus zeigt diese Anzeige die Summe der Standalone ONTAP SVMs und Cluster ONTAP SVMs, die von SnapCenter verwaltet werden und auf die Sie Zugriff haben. Wenn Sie auf die Zahl neben SVM klicken, werden Sie auf die Seite „Speichersysteme“ weitergeleitet. Von dort aus können Sie detaillierte Informationen zu einem ausgewählten SVM erhalten.

Der Hostkonfigurationsstatus wird zusammen mit der Anzahl der Hosts in jedem Status als Rot (kritisch), Gelb (Warnung) und Grün (aktiv) angezeigt. Für jeden Zustand werden Statusmeldungen bereitgestellt.

| Konfigurationsstatus                      | Beschreibung                                                                                                                                                                    |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade obligatorisch                     | Anzahl der Hosts, die nicht unterstützte Plug-Ins ausführen und ein Upgrade benötigen. Ein nicht unterstütztes Plug-In ist mit dieser Version von SnapCenter nicht kompatibel.  |
| Migration obligatorisch                   | Anzahl der Hosts, die nicht unterstützte Plug-Ins ausführen und migriert werden müssen. Ein nicht unterstütztes Plug-In ist mit dieser Version von SnapCenter nicht kompatibel. |
| Keine Plug-Ins installiert                | Anzahl der Hosts, die erfolgreich hinzugefügt wurden, bei denen aber die Plug-Ins installiert werden müssen oder bei denen die Plug-In-Installation fehlgeschlagen ist.         |
| Ausgesetzt                                | Anzahl der Hosts, deren Zeitpläne ausgesetzt sind und gewartet werden.                                                                                                          |
| Gestoppt                                  | Anzahl der Hosts, die aktiv sind, deren Plug-In-Dienste jedoch nicht ausgeführt werden.                                                                                         |
| Host ausgefallen                          | Anzahl der Hosts, die ausgefallen oder nicht erreichbar sind.                                                                                                                   |
| Upgrade verfügbar (optional)              | Anzahl der Hosts, für die eine neuere Version des Plug-In-Pakets zum Upgrade verfügbar ist.                                                                                     |
| Migration verfügbar (optional)            | Anzahl der Hosts, für die eine neuere Version des Plug-Ins zur Migration verfügbar ist.                                                                                         |
| Konfigurieren des Protokollverzeichnisses | Anzahl der Hosts, bei denen das Protokollverzeichnis für SCSQL konfiguriert werden muss, um eine Transaktionsprotokollsicherung durchzuführen.                                  |

| Konfigurationsstatus                     | Beschreibung                                                                                                                          |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Konfigurieren von VMware-Plug-Ins        | Anzahl der Hosts, denen das SnapCenter Plug-in for VMware vSphere hinzugefügt werden muss.                                            |
| Unbekannt                                | Anzahl der Hosts, die registriert wurden, deren Installation jedoch noch nicht ausgelöst wurde.                                       |
| Wird ausgeführt                          | Anzahl der aktiven Hosts und ausgeführten Plug-Ins. Und im Fall von SCSQL-Plugins werden Log-Verzeichnis und Hypervisor konfiguriert. |
| Installieren/Deinstallieren von Plug-Ins | Anzahl der Hosts, auf denen die Plug-In-Installation oder -Deinstallation läuft.                                                      |

## So zeigen Sie Informationen auf dem Dashboard an

Im linken Navigationsbereich von SnapCenter können Sie verschiedene Dashboard-Kacheln oder Anzeigen zusammen mit den zugehörigen Systemdetails anzeigen. Die Anzahl der im Dashboard verfügbaren Anzeigen ist festgelegt und kann nicht geändert werden. Der in jeder Anzeige bereitgestellte Inhalt hängt von der rollenbasierten Zugriffskontrolle (RBAC) ab.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Klicken Sie auf die aktiven Bereiche auf jedem Display, um zusätzliche Informationen zu erhalten.

Wenn Sie beispielsweise in **Jobs** auf ein Ringdiagramm klicken, werden Sie auf die Monitorseite weitergeleitet, wo Sie weitere Informationen zu Ihrer Auswahl erhalten. Wenn Sie in der **Schutzzusammenfassung** auf ein Ringdiagramm klicken, werden Sie auf die Seite „Berichte“ weitergeleitet, auf der Sie weitere Informationen zu Ihrer Auswahl erhalten.

## Fordern Sie Statusberichte der Jobs vom Dashboard an

Sie können auf der Dashboard-Seite Berichte zu Sicherungs-, Wiederherstellungs- und Klonaufträgen anfordern. Dies ist nützlich, wenn Sie die Gesamtzahl der erfolgreichen oder fehlgeschlagenen Jobs in Ihrer SnapCenter -Umgebung ermitteln möchten.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**
2. Suchen Sie im Dashboard nach der Kachel „Jobs“ und wählen Sie dann **Backup**, **Wiederherstellen** oder **Klonen**.
3. Wählen Sie mithilfe des Pulldown-Menüs den Zeitraum aus, für den Sie Jobinformationen wünschen: 24 Stunden, 7 Tage oder 30 Tage.

Die Systeme zeigen ein Donut-Diagramm an, das die Daten abdeckt.

4. Klicken Sie auf das Donut-Segment, das die Auftragsinformationen darstellt, für die Sie einen Bericht wünschen.

Wenn Sie auf das Ringdiagramm klicken, werden Sie von der Dashboard-Seite zur Monitor-Seite weitergeleitet. Auf der Seite „Überwachen“ werden die Jobs mit dem Status angezeigt, den Sie im Ringdiagramm ausgewählt haben.

5. Klicken Sie in der Liste der Monitorseite auf einen bestimmten Job, um ihn auszuwählen.
6. Klicken Sie oben auf der Monitorseite auf **Berichte**.

## Ergebnis

Der Bericht zeigt nur Informationen zu dem von Ihnen ausgewählten Job an. Sie können den Bericht überprüfen oder auf Ihr lokales System herunterladen.

## Fordern Sie Berichte zum Schutzstatus vom Dashboard an

Sie können über das Dashboard Schutzdetails für Ressourcen anfordern, die von bestimmten Plug-ins verwaltet werden. Für die Datenschutzzusammenfassung werden ausschließlich Datensicherungen berücksichtigt.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Suchen Sie im Dashboard nach der Kachel „Neueste Schutzzusammenfassung“ und wählen Sie über das Pulldown-Menü ein Plug-In aus.

Das Dashboard zeigt ein Ringdiagramm für im primären Speicher gesicherte Ressourcen und, falls für das Plug-In zutreffend, ein Ringdiagramm für im sekundären Speicher gesicherte Ressourcen an.



Datenschutzberichte sind nur für bestimmte Plug-In-Typen verfügbar. Die Angabe von **Alle Plug-ins** wird nicht unterstützt.

3. Klicken Sie auf das Donut-Segment, das den Status darstellt, für den Sie einen Bericht wünschen.

Wenn Sie auf das Ringdiagramm klicken, werden Sie von der Dashboard-Seite zu den Berichten und dann zur Plug-in-Seite weitergeleitet. Der Bericht zeigt nur den Status für das von Ihnen ausgewählte Plug-In an. Sie können den Bericht überprüfen oder auf Ihr lokales System herunterladen.



Die Umleitung zur Berichtsseite für SnapMirror -Ringdiagramme und dateibasierte SAP HANA-Sicherungen wird nicht unterstützt.

## RBAC verwalten

Mit SnapCenter können Sie Rollen, Benutzer und Gruppen ändern.

### Ändern einer Rolle

Sie können eine SnapCenter -Rolle ändern, um Benutzer oder Gruppen zu entfernen und die mit der Rolle verknüpften Berechtigungen zu ändern. Das Ändern von Rollen ist besonders dann sinnvoll, wenn Sie die von

einer ganzen Rolle verwendeten Berechtigungen ändern oder entfernen möchten.

### Bevor Sie beginnen

Sie müssen sich mit der Rolle „SnapCenterAdmin“ angemeldet haben.



Sie können die Berechtigungen für die Rolle „SnapCenterAdmin“ weder ändern noch entfernen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Rollen**.
3. Klicken Sie im Feld „Rollenname“ auf die Rolle, die Sie ändern möchten.
4. Wählen Sie **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen** aus, um anderen Mitgliedern der Rolle das Anzeigen von Ressourcen wie Volumes und Hosts zu ermöglichen, nachdem sie die Ressourcenliste aktualisiert haben.

Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Mitglieder dieser Rolle Objekte sehen, denen andere Mitglieder zugewiesen sind.



Wenn diese Option aktiviert ist, ist es nicht erforderlich, Benutzern Zugriff auf Objekte oder Ressourcen zuzuweisen, wenn die Benutzer derselben Rolle angehören wie der Benutzer, der die Objekte oder Ressourcen erstellt hat.

5. Ändern Sie auf der Seite „Rollendetails“ die Berechtigungen oder heben Sie die Zuweisung der Mitglieder nach Bedarf auf.
6. Klicken Sie auf **Senden**.

## Benutzer und Gruppen ändern

Sie können SnapCenter Benutzer oder -Gruppen ändern, um ihre Rollen und Ressourcen zu verändern.

### Bevor Sie beginnen

Sie müssen als SnapCenter Administrator angemeldet sein.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Benutzer und Zugriff**.
3. Klicken Sie in der Liste „Benutzer- oder Gruppenname“ auf den Benutzer oder die Gruppe, den/die Sie ändern möchten.
4. Ändern Sie auf der Benutzer- oder Gruppendetailseite Rollen und Assets.
5. Klicken Sie auf **Senden**.

## Hosts verwalten

Sie können Hosts hinzufügen und SnapCenter Plug-In-Pakete installieren, einen Verifizierungsserver hinzufügen, Hosts entfernen, Sicherungsaufträge migrieren und Hosts aktualisieren, um Plug-In-Pakete zu aktualisieren oder neue Plug-In-Pakete

hinzuzufügen. Je nach verwendetem Plug-In können Sie auch Datenträger bereitstellen, SMB-Freigaben verwalten, Initiatorgruppen (igroups) verwalten, iSCSI-Sitzungen verwalten und Daten migrieren.

| Sie können diese Aufgaben ausführen...                                        | Für Microsoft Exchange Server | Für Microsoft SQL Server | Für Microsoft Windows | Für Oracle-Datenbanken | Für SAP HANA-Datenbank | Für NetApp unterstützte Plug-Ins | Für Db2 | Für PostgreSQL | Für MySQL |
|-------------------------------------------------------------------------------|-------------------------------|--------------------------|-----------------------|------------------------|------------------------|----------------------------------|---------|----------------|-----------|
| Hosts hinzufügen und Plug-In-Paket installieren                               | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     | Ja                               | Ja      | Ja             | Ja        |
| Aktualisieren der ESXi-Informationen für einen Host                           | Nein                          | Ja                       | Nein                  | Nein                   | Nein                   | Nein                             | Nein    | Nein           | Nein      |
| Zeitpläne aussetzen und Hosts in den Wartungsmodus versetzen                  | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     | Ja                               | Ja      | Ja             | Ja        |
| Ändern Sie Hosts, indem Sie Plug-Ins hinzufügen, aktualisieren oder entfernen | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     | Ja                               | Ja      | Ja             | Ja        |

| Sie können diese Aufgaben ausführen...                                                        | Für Microsoft Exchange Server | Für Microsoft SQL Server | Für Microsoft Windows | Für Oracle-Datenbanken | Für SAP HANA-Datenbanken | Für NetApp unterstützte Plug-Ins | Für Db2 | Für PostgreSQL | Für MySQL |
|-----------------------------------------------------------------------------------------------|-------------------------------|--------------------------|-----------------------|------------------------|--------------------------|----------------------------------|---------|----------------|-----------|
| Hosts aus SnapCenter entfernen                                                                | Ja                            | Ja                       | Ja                    | Ja                     | Ja                       | Ja                               | Ja      | Ja             | Ja        |
| Plug-In-Dienste starten (gilt nur für Plug-Ins, die auf einem Windows-Host ausgeführt werden) | Ja                            | Ja                       | Ja                    | Nein                   | Ja                       | Ja                               | Ja      | Ja             | Ja        |
| Bereitstellen von Datenträgern                                                                | Nein                          | Nein                     | Ja                    | Nein                   | Nein                     | Nein                             | Nein    | Nein           | Nein      |
| Verwalten von SMB-Freigaben                                                                   | Nein                          | Nein                     | Ja                    | Nein                   | Nein                     | Nein                             | Nein    | Nein           | Nein      |
| iGroups verwalten                                                                             | Nein                          | Nein                     | Ja                    | Nein                   | Nein                     | Nein                             | Nein    | Nein           | Nein      |
| Verwalten von iSCSI-Sitzungen                                                                 | Nein                          | Nein                     | Ja                    | Nein                   | Nein                     | Nein                             | Nein    | Nein           | Nein      |

## Aktualisieren der Informationen zur virtuellen Maschine

Sie sollten die Informationen Ihrer virtuellen Maschine aktualisieren, wenn sich die Anmeldeinformationen für

VMware vCenter ändern oder der Datenbank- oder Dateisystemhost neu gestartet wird. Durch das Aktualisieren Ihrer virtuellen Maschineninformationen in SnapCenter wird die Kommunikation mit dem VMware vSphere vCenter initiiert und die vCenter-Anmeldeinformationen abgerufen.



RDM-basierte Festplatten werden vom SnapCenter -Plug-in für Microsoft Windows verwaltet, das auf dem Datenbankhost installiert ist. Zur Verwaltung von RDMs kommuniziert das SnapCenter -Plug-in für Microsoft Windows mit dem vCenter-Server, der den Datenbankhost verwaltet.

## Schritte

1. Klicken Sie im linken Navigationsbereich von SnapCenter auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, den Sie aktualisieren möchten.
4. Klicken Sie auf **VM aktualisieren**.

## Plug-In-Hosts ändern

Nach der Installation eines Plug-Ins können Sie die Details des Plug-In-Hosts bei Bedarf ändern. Sie können Anmeldeinformationen, Installationspfad, Plug-Ins, Protokollverzeichnisdetails für das SnapCenter -Plug-In für Microsoft SQL Server, das gruppenverwaltete Dienstkonto (gMSA) und den Plug-In-Port ändern.



Stellen Sie sicher, dass die Plug-in-Version mit der SnapCenter Server-Version übereinstimmt.

## Über diese Aufgabe

- Sie können einen Plug-In-Port erst ändern, nachdem das Plug-In installiert wurde.

Während der Ausführung von Upgrade-Vorgängen können Sie den Plug-In-Port nicht ändern.

- Beim Ändern eines Plug-In-Ports sollten Sie sich der folgenden Port-Rollback-Szenarien bewusst sein:
  - Wenn SnapCenter in einer eigenständigen Konfiguration den Port einer der Komponenten nicht ändern kann, schlägt der Vorgang fehl und der alte Port wird für alle Komponenten beibehalten.

Wurde der Port bei allen Komponenten geändert, eine Komponente startet jedoch nicht mit dem neuen Port, bleibt der alte Port bei allen Komponenten erhalten. Wenn Sie beispielsweise den Port für zwei Plug-Ins auf dem eigenständigen Host ändern möchten und SnapCenter den neuen Port nicht auf eines der Plug-Ins anwenden kann, schlägt der Vorgang fehl (mit einer entsprechenden Fehlermeldung) und der alte Port wird für beide Plug-Ins beibehalten.

- Wenn SnapCenter in einer Clusterkonfiguration den Port des auf einem der Knoten installierten Plug-Ins nicht ändern kann, schlägt der Vorgang fehl und der alte Port wird für alle Knoten beibehalten.

Wenn das Plug-In beispielsweise auf vier Knoten in einer Clusterkonfiguration installiert ist und der Port für einen der Knoten nicht geändert wird, bleibt der alte Port für alle Knoten erhalten.

Wenn Plug-Ins mit gMSA installiert werden, können Sie im Fenster **Weitere Optionen** Änderungen vornehmen. Wenn Plug-Ins ohne gMSA installiert werden, können Sie das gMSA-Konto angeben, um es als Plug-In-Dienstkonto zu verwenden.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Wählen Sie den Host aus, für den Sie Änderungen vornehmen möchten, und ändern Sie ein beliebiges Feld.

Es kann immer nur ein Feld gleichzeitig geändert werden.

4. Klicken Sie auf **Senden**.

## Ergebnis

Der Host wird validiert und zum SnapCenter -Server hinzugefügt.

## Starten oder Neustarten von Plug-In-Diensten

Durch das Starten der SnapCenter Plug-In-Dienste können Sie Dienste starten, wenn sie nicht ausgeführt werden, oder sie neu starten, wenn sie ausgeführt werden. Möglicherweise möchten Sie die Dienste nach der Durchführung der Wartung neu starten.

Sie sollten sicherstellen, dass beim Neustart der Dienste keine Jobs ausgeführt werden.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, den Sie starten möchten.
4. Klicken  Symbol und klicken Sie auf **Dienst starten** oder **Dienst neu starten**.

Sie können den Dienst mehrerer Hosts gleichzeitig starten oder neu starten.

## Zeitpläne für Host-Wartung aussetzen

Wenn Sie verhindern möchten, dass der Host geplante SnapCenter -Jobs ausführt, können Sie Ihren Host in den Wartungsmodus versetzen. Sie sollten dies tun, bevor Sie die Plug-Ins aktualisieren oder wenn Sie Wartungsaufgaben auf Hosts durchführen.



Sie können die Zeitpläne auf einem ausgefallenen Host nicht anhalten, da SnapCenter nicht mit diesem Host kommunizieren kann.

## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, den Sie sperren möchten.
4. Klicken Sie auf das  und klicken Sie dann auf **Zeitplan anhalten**, um den Host für dieses Plug-In in den Wartungsmodus zu versetzen.

Sie können den Zeitplan mehrerer Hosts gleichzeitig aussetzen.





Sie müssen den Plug-In-Dienst nicht zuerst beenden. Der Plug-In-Dienst kann ausgeführt oder gestoppt werden.

## Ergebnis

Nachdem Sie die Zeitpläne auf dem Host ausgesetzt haben, wird auf der Seite „Verwaltete Hosts“ im Feld „Gesamtstatus“ für den Host der Eintrag **Ausgesetzt** angezeigt.

Nachdem Sie die Hostwartung abgeschlossen haben, können Sie den Host aus dem Wartungsmodus holen, indem Sie auf **Zeitplan aktivieren** klicken. Sie können den Zeitplan mehrerer Hosts gleichzeitig aktivieren.

## Von der Seite „Ressourcen“ unterstützte Vorgänge

Auf der Seite „Ressourcen“ können Sie Ressourcen ermitteln und Datenschutzvorgänge durchführen. Die Vorgänge, die Sie ausführen können, unterscheiden sich je nach dem Plug-In, das Sie zum Verwalten Ihrer Ressourcen verwenden.

Auf der Seite „Ressourcen“ können Sie die folgenden Aufgaben ausführen:

| Sie können diese Aufgaben ausführen...                     | Für Microsoft Exchange Server | Für Microsoft SQL Server | Für Microsoft Windows | Für Oracle-Datenbanken | Für SAP HANA-Datenbank |
|------------------------------------------------------------|-------------------------------|--------------------------|-----------------------|------------------------|------------------------|
| Ermitteln, ob Ressourcen für die Sicherung verfügbar sind  | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     |
| Führen Sie bei Bedarf eine Sicherung einer Ressource durch | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     |
| Wiederherstellen aus Backups                               | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     |
| Klonen von Backups                                         | Nein                          | Ja                       | Ja                    | Ja                     | Ja                     |
| Backups verwalten                                          | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     |
| Verwalten von Klonen                                       | Nein                          | Ja                       | Ja                    | Ja                     | Ja                     |
| Richtlinien verwalten                                      | Ja                            | Ja                       | Ja                    | Ja                     | Ja                     |

| <b>Sie können diese Aufgaben ausführen...</b> | <b>Für Microsoft Exchange Server</b> | <b>Für Microsoft SQL Server</b> | <b>Für Microsoft Windows</b> | <b>Für Oracle-Datenbanken</b> | <b>Für SAP HANA-Datenbank</b> |
|-----------------------------------------------|--------------------------------------|---------------------------------|------------------------------|-------------------------------|-------------------------------|
| Speicherverbindungen verwalten                | Ja                                   | Ja                              | Ja                           | Ja                            | Ja                            |
| Mounten von Backups                           | Nein                                 | Nein                            | Nein                         | Ja                            | Nein                          |
| Sicherungen aushängen                         | Nein                                 | Nein                            | Nein                         | Ja                            | Nein                          |
| Details anzeigen                              | Ja                                   | Ja                              | Ja                           | Ja                            | Ja                            |

## Richtlinien verwalten

Sie können Richtlinien von einer Ressource oder Ressourcengruppe trennen, ändern, löschen, anzeigen und kopieren.

### Richtlinien ändern

Sie können die Replikationsoptionen, die Einstellungen für die Snapshot-Aufbewahrung, die Anzahl der Wiederholungsversuche bei Fehlern oder die Skriptinformationen ändern, während eine Richtlinie an eine Ressource oder Ressourcengruppe angehängt ist. Sie können den Zeitplantyp (Häufigkeit) erst ändern, nachdem Sie eine Richtlinie getrennt haben.

### Über diese Aufgabe

Das Ändern des Zeitplantyps in einer Richtlinie erfordert zusätzliche Schritte, da der SnapCenter Server den Zeitplantyp nur zu dem Zeitpunkt registriert, zu dem die Richtlinie einer Ressource oder Ressourcengruppe zugeordnet wird.

| <b>Wenn Sie wollen...</b>                 | <b>Dann...</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Einen zusätzlichen Zeitplantyp hinzufügen | <p>Erstellen Sie eine neue Richtlinie und hängen Sie sie an die erforderlichen Ressourcen oder Ressourcengruppen an.</p> <p>Wenn beispielsweise eine Ressourcengruppenrichtlinie nur stündliche Sicherungen vorgibt und Sie auch tägliche Sicherungen hinzufügen möchten, können Sie eine Richtlinie mit einem täglichen Zeitplantyp erstellen und sie der Ressourcengruppe hinzufügen. Die Ressourcengruppe hätte dann zwei Richtlinien: stündlich und täglich.</p> |

| Wenn Sie wollen...                       | Dann...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entfernen oder Ändern eines Zeitplantyps | <p>Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Trennen Sie die Richtlinie von jeder Ressource und Ressourcengruppe, die diese Richtlinie verwendet.</li> <li>2. Ändern Sie den Zeitplantyp.</li> <li>3. Fügen Sie die Richtlinie erneut allen Ressourcen und Ressourcengruppen hinzu.</li> </ol> <p>Wenn beispielsweise eine Richtlinie stündliche Sicherungen vorsieht und Sie diese in tägliche Sicherungen ändern möchten, müssen Sie die Richtlinie zuerst trennen.</p> |

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie die Richtlinie aus und klicken Sie dann auf **Ändern**.
4. Ändern Sie die Informationen und klicken Sie dann auf **Fertig**.

## Richtlinien trennen

Sie können Richtlinien jederzeit von einer Ressource oder Ressourcengruppe trennen, wenn Sie nicht mehr möchten, dass diese Richtlinien den Datenschutz für die Ressourcen regeln. Sie müssen eine Richtlinie trennen, bevor Sie sie löschen oder den Zeitplantyp ändern können.

### 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 „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie dann auf **Ressourcengruppe ändern**.
4. Deaktivieren Sie auf der Seite „Richtlinien“ des Assistenten „Ressourcengruppe ändern“ in der Dropdownliste das Häkchen neben den Richtlinien, die Sie trennen möchten.
5. Nehmen Sie im Rest des Assistenten weitere Änderungen an der Ressourcengruppe vor und klicken Sie dann auf **Fertig**.

## Richtlinien löschen

Wenn Sie Richtlinien nicht mehr benötigen, möchten Sie sie möglicherweise löschen.

### Bevor Sie beginnen

Sie sollten die Richtlinie von Ressourcen oder Ressourcengruppen trennen, wenn die Richtlinie mit Ressourcen oder Ressourcengruppen verknüpft ist.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie die Richtlinie aus und klicken Sie dann auf **Löschen**.
4. Klicken Sie auf **Ja**.

## Verwalten von Ressourcengruppen

Sie können verschiedene Vorgänge an Ressourcengruppen durchführen.

Sie können die folgenden Aufgaben im Zusammenhang mit Ressourcengruppen ausführen:

- Ändern Sie eine Ressourcengruppe, indem Sie die Ressourcengruppe auswählen und auf **Ressourcengruppe ändern** klicken, um die Informationen zu bearbeiten, die Sie beim Erstellen der Ressourcengruppe angegeben haben.



Sie können den Zeitplan ändern, während Sie die Ressourcengruppe ändern. Um den Zeitplantyp zu ändern, müssen Sie jedoch die Richtlinie ändern.



Wenn Sie Ressourcen aus einer Ressourcengruppe entfernen, werden die in den aktuell mit der Ressourcengruppe verknüpften Richtlinien definierten Einstellungen zur Sicherungsaufbewahrung weiterhin auf die entfernten Ressourcen angewendet.

- Erstellen Sie eine Sicherung einer Ressourcengruppe.
- Erstellen Sie einen Klon einer Sicherung.

Sie können aus den vorhandenen Sicherungen von SQL, Oracle, Windows-Dateisystemen, benutzerdefinierten Anwendungen und SAP HANA-Datenbankressourcen oder -Ressourcengruppen klonen.

- Erstellen Sie einen Klon einer Ressourcengruppe.

Dieser Vorgang wird nur für SQL-Ressourcengruppen unterstützt (die nur Datenbanken enthalten). Sie können einen Zeitplan zum Klonen einer Ressourcengruppe (Klon-Lebenszyklus) konfigurieren.

- Verhindern Sie, dass geplante Vorgänge für Ressourcengruppen gestartet werden.
- Löschen Sie eine Ressourcengruppe.

## Stoppen und Fortsetzen von Vorgängen für Ressourcengruppen

Sie können den Start geplanter Vorgänge für eine Ressourcengruppe vorübergehend deaktivieren. Sie können diese Vorgänge später bei Bedarf aktivieren.

### 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 „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie auf **Wartung**.
4. Klicken Sie auf **OK**.

Wenn Sie den Betrieb der Ressourcengruppe fortsetzen möchten, die Sie in den Wartungsmodus versetzt haben, wählen Sie die Ressourcengruppe aus und klicken Sie auf **Produktion**.

## Ressourcengruppen löschen

Sie können eine Ressourcengruppe löschen, wenn Sie die Ressourcen in der Ressourcengruppe nicht mehr schützen müssen. Sie müssen sicherstellen, dass Ressourcengruppen gelöscht werden, bevor Sie Plug-Ins aus SnapCenter entfernen.

### Über diese Aufgabe

Sie sollten alle für eine der Ressourcen in der Ressourcengruppe erstellten Klone manuell löschen. Sie können optional das Löschen aller mit der Ressourcengruppe verknüpften Sicherungen, Metadaten, Richtlinien und Snapshots erzwingen.

### 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 „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie dann auf **Löschen**.
4. Optional: Aktivieren Sie das Kontrollkästchen **Mit dieser Ressourcengruppe verknüpfte Sicherungen löschen und Richtlinien trennen**, um alle mit der Ressourcengruppe verknüpften Sicherungen, Metadaten, Richtlinien und Snapshots zu entfernen.
5. Klicken Sie auf **OK**.

## Backups verwalten

Sie können Backups umbenennen und löschen. Sie können auch mehrere Backups gleichzeitig löschen.

### Backups umbenennen

Sie können Sicherungen umbenennen, wenn Sie einen besseren Namen angeben möchten, um die Suchbarkeit zu verbessern.

### 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 oder Ressourcengruppe aus der Liste aus.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt. Wenn die Ressource oder Ressourcengruppe nicht für den Datenschutz konfiguriert ist, wird anstelle der Topologieseite der Schutzassistent angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus den primären Speichersystemen aus.

Sie können die Sicherungen, die sich auf dem sekundären Speichersystem befinden, nicht umbenennen.

Wenn Sie die Sicherungen von Oracle-Datenbanken mit Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Sicherungen nicht umbenennen.

5. Wählen Sie die Sicherung aus und klicken Sie dann auf .
6. Geben Sie im Feld **Backup umbenennen in** einen neuen Namen ein und klicken Sie auf **OK**.

## Backups löschen

Sie können Sicherungen löschen, wenn Sie die Sicherung für andere Datenschutzvorgänge nicht mehr benötigen.

### Bevor Sie beginnen

Vor dem Löschen eines Backups müssen Sie die zugehörigen Klone gelöscht haben.



Wenn eine Sicherung mit einer geklonten Ressource verknüpft ist, können Sie die Sicherung nicht löschen.

### 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 oder Ressourcengruppe aus der Liste aus.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus den primären Speichersystemen aus.

Sie können die Sicherungen, die sich auf dem sekundären Speichersystem befinden, nicht löschen.

5. Wählen Sie die Sicherung aus und klicken Sie dann auf .

Wenn Sie eine SAP HANA-Datenbanksicherung löschen, werden auch die zugehörigen SAP HANA-Kataloge der Sicherung gelöscht.



Wenn die letzte verbleibende Sicherung gelöscht wird, können die zugehörigen HANA-Katalogeinträge nicht gelöscht werden.

6. Klicken Sie auf **OK**.



Wenn Sie in SnapCenter über veraltete Datenbanksicherungen verfügen, für die es keine entsprechenden Sicherungen auf dem Speichersystem gibt, müssen Sie den Befehl „remove-smbbackup“ verwenden, um diese veralteten Sicherungseinträge zu bereinigen. Wenn die veralteten Sicherungen katalogisiert wurden, werden sie aus der Wiederherstellungskatalogdatenbank dekatalogisiert.

## Schutz entfernen

Durch Entfernen des Schutzes werden alle Sicherungen gelöscht und alle Richtlinien getrennt. Bevor Sie den

Schutz entfernen, sollten Sie sicherstellen, dass die Sicherungen nicht gemountet sind und keine Klone mit der Sicherung verknüpft sind.

### 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 oder Ressourcengruppe aus der Liste aus.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie die Sicherung aus und klicken Sie auf **Schutz entfernen**.

## Klone löschen

Sie können Klone löschen, wenn Sie sie nicht mehr benötigen.

### Über diese Aufgabe

Sie können keine Klone löschen, die als Quelle für andere Klone fungieren.

Wenn die Produktionsdatenbank beispielsweise db1 ist, wird die Datenbank clone1 aus der Sicherung von db1 geklont und anschließend clone1 geschützt. Die Datenbank „Klon2“ wird aus der Sicherung von „Klon1“ geklont. Wenn Sie Klon1 löschen möchten, müssen Sie zuerst Klon2 und dann Klon1 löschen.

### 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 oder Ressourcengruppe aus der Liste aus.

Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Klone** entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
5. Wählen Sie den Klon aus und klicken Sie dann auf .

Wenn Sie SAP HANA-Datenbankklone löschen, führen Sie auf der Seite „Klone löschen“ die folgenden Aktionen aus:

- a. Geben Sie im Feld **Pre clone delete** die Befehle ein, die vor dem Löschen des Klons ausgeführt werden sollen.
  - b. Geben Sie im Feld **Unmount** den Befehl zum Unmounten des Klons ein, bevor Sie ihn löschen.
6. Klicken Sie auf **OK**.

### Nachdem Sie fertig sind

Manchmal werden die Dateisysteme nicht gelöscht. Sie müssen den Wert des Parameters `CLONE_DELETE_DELAY` erhöhen, indem Sie den folgenden Befehl ausführen: `./sccli Set-SmConfigSettings`



Der Parameter `CLONE_DELETE_DELAY` gibt die Anzahl der Sekunden an, die nach Abschluss des Löschsens des Anwendungsklons gewartet werden soll, bevor mit dem Löschen des Dateisystems begonnen wird.

Starten Sie den SnapCenter Plug-in Loader (SPL)-Dienst neu, nachdem Sie den Wert des Parameters geändert haben.

## Überwachen Sie Jobs, Zeitpläne, Ereignisse und Protokolle

Auf der Seite „Überwachen“ können Sie den Fortschritt Ihrer Jobs überwachen, Informationen zu geplanten Jobs abrufen und Ereignisse und Protokolle überprüfen.

### Überwachen von Jobs

Sie können Informationen zu SnapCenter -Sicherungs-, Klon-, Wiederherstellungs- und Überprüfungsaufträgen anzeigen. Sie können diese Ansicht nach Start- und Enddatum, Auftragstyp, Ressourcengruppe, Richtlinie oder SnapCenter -Plug-in filtern. Sie können auch zusätzliche Details und Protokolldateien für bestimmte Aufträge abrufen.

Sie können auch Jobs im Zusammenhang mit SnapMirror und SnapVault -Vorgängen überwachen.



Sie können nur die Jobs überwachen, die Sie erstellt haben und die für Sie relevant sind, es sei denn, Ihnen wird die Rolle „SnapCenter -Administrator“ oder eine andere Superuser-Rolle zugewiesen.

Sie können die folgenden Aufgaben im Zusammenhang mit der Überwachung von Jobs ausführen:

- Überwachen Sie Sicherungs-, Klon-, Wiederherstellungs- und Überprüfungsvorgänge.
- Zeigen Sie Auftragsdetails und Berichte an.
- Stoppen Sie einen geplanten Job.

### Verwalten geplanter Sicherungsaufträge

Ab der Version SnapCenter 6.0.1 wurde ein neuer Parameter **JobConcurrencyThreshold** eingeführt, der einen Schwellenwert für die Anzahl der geplanten Jobs festlegt, die zu einem bestimmten Zeitpunkt ausgeführt werden können. Auf diese Weise können Sie die Anzahl der Sicherungen, die Sie ausführen möchten, basierend auf der Hardwarekonfiguration Ihres Systems steuern.

Der **JobConcurrencyThreshold** zugewiesene Standardwert ist 0 und ist deaktiviert. Sie können die Funktion aktivieren, indem Sie einen Wert zuweisen, wenn Sie während des geplanten Sicherungsfensters eine Leistungsver schlechterung feststellen.



Wenn Sie **JobConcurrencyThreshold** aktivieren, um gleichzeitige Jobs zu verwalten, können Sie mit SnapCenter die Reihenfolge der Sicherungen nicht steuern und die Sicherungen werden möglicherweise nicht zum im Zeitplan angegebenen Zeitpunkt ausgelöst.

### Schritte



1. Legen Sie den Wert des Parameters *JobConcurrencyThreshold* fest, der sich unter \_C:\Programme\NetApp\ SnapCenter WebApp\ SnapManager befindet.
2. Starten Sie den SnapCenter -Anwendungspool neu, indem Sie auf IIS > Anwendungspools > SnapCenter > Neustart klicken.
3. Starten Sie den SnapCenter -Webdienst neu, indem Sie auf IIS > Sites > SnapCenter > Neustart klicken.

## Verwalten veralteter Jobs

Veraltete Jobs entstehen durch Unterbrechungen in SnapCenter oder durch unsachgemäße Job-Updates. Ab der Version SnapCenter 6.0.1 wird ein vordefinierter Zeitplan eingeführt, um diese veralteten Jobs zu bereinigen, die länger als 72 Stunden feststecken. Sie können die Zeitplanhäufigkeit ändern, indem Sie den konfigurierbaren Parameter **CleanUpStaleJobsIntervalHours** bearbeiten.

Sie können die Bereinigung bei Bedarf auslösen, indem Sie den Zeitplan unter **Monitor > Zeitpläne > SnapCenter\_StaleJobCleanUp** ausführen.

### Schritte

1. Legen Sie den Wert des Parameters *CleanUpStaleJobsIntervalHours* fest, der sich unter \_C:\Programme\NetApp\ SnapCenter WebApp\ SnapManager befindet.
2. Starten Sie den SnapCenter -Anwendungspool neu, indem Sie auf IIS > Anwendungspools > SnapCenter > Neustart klicken.
3. Starten Sie den SnapCenter -Webdienst neu, indem Sie auf IIS > Sites > SnapCenter > Neustart klicken.

## Zeitpläne überwachen

Möglicherweise möchten Sie aktuelle Zeitpläne anzeigen, um festzustellen, wann der Vorgang beginnt, wann er zuletzt ausgeführt wurde und wann er das nächste Mal ausgeführt wird. Sie können außerdem den Host bestimmen, auf dem der Vorgang ausgeführt wird, sowie die Ressourcengruppe und Richtlinieninformationen des Vorgangs.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Zeitpläne**.
3. Wählen Sie die Ressourcengruppe und den Zeitplantyp aus.
4. Zeigen Sie die Liste der geplanten Vorgänge an.

## Überwachen von Ereignissen

Sie können eine Liste der SnapCenter -Ereignisse im System anzeigen, z. B. wenn ein Benutzer eine Ressourcengruppe erstellt oder wenn das System Aktivitäten initiiert, z. B. das Erstellen einer geplanten Sicherung. Möglicherweise möchten Sie Ereignisse anzeigen, um festzustellen, ob gerade ein Vorgang wie beispielsweise eine Sicherung oder Wiederherstellung ausgeführt wird.

### Über diese Aufgabe

Alle Jobinformationen werden auf der Seite „Ereignisse“ angezeigt. Wenn beispielsweise ein Sicherungsauftrag gestartet wird, wird ein Ereignis „Sicherungsstart“ angezeigt. Wenn die Sicherung abgeschlossen ist, wird das Ereignis „Sicherung abgeschlossen“ angezeigt.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Ereignisse**.
3. (Optional) Geben Sie im Feld „Filter“ das Start- oder Enddatum, die Ereigniskategorie (z. B. Sicherung, Ressourcengruppe oder Richtlinie) und den Schweregrad ein und klicken Sie auf „Übernehmen“. Alternativ können Sie Zeichen in das Suchfeld eingeben.
4. Sehen Sie sich die Liste der Ereignisse an.

## Überwachen von Protokollen

Sie können SnapCenter -Serverprotokolle, SnapCenter Host-Agent-Protokolle und Plug-In-Protokolle anzeigen und herunterladen. Möglicherweise möchten Sie die Protokolle zur Unterstützung bei der Fehlerbehebung anzeigen.

### Über diese Aufgabe

Sie können die Protokolle filtern, um nur einen bestimmten Protokollschweregrad anzuzeigen:

- Debuggen
- Info
- Warnen
- Fehler
- Tödlich

Sie können auch Protokolle auf Auftragsebene abrufen, beispielsweise Protokolle, die Ihnen bei der Fehlerbehebung bei einem fehlgeschlagenen Sicherungsauftrag helfen. Verwenden Sie für Protokolle auf Jobebene die Option **Monitor > Jobs**.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Wählen Sie auf der Seite „Jobs“ einen Job aus und klicken Sie auf „Protokolle herunterladen“.

Der heruntergeladene ZIP-Ordner enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des komprimierten Ordners enthält die Job-ID und den ausgewählten Jobtyp.

3. Klicken Sie auf der Seite „Überwachen“ auf **Protokolle**.
4. Wählen Sie den Protokolltyp, den Host und die Instanz aus.

Wenn Sie den Protokolltyp „Plugin“ auswählen, können Sie ein Host- oder SnapCenter -Plugin auswählen. Dies ist nicht möglich, wenn der Protokolltyp „Server“ ist.

5. Um die Protokolle nach einer bestimmten Quelle, Nachricht oder Protokollebene zu filtern, klicken Sie auf das Filtersymbol oben in der Spaltenüberschrift.

Um alle Protokolle anzuzeigen, wählen Sie **Größer als oder gleich** als Debug Ebene.

6. Klicken Sie auf **Aktualisieren**.
7. Zeigen Sie die Liste der Protokolle an.
8. Klicken Sie auf **Herunterladen**, um die Protokolle herunterzuladen.

Der heruntergeladene ZIP-Ordner enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des komprimierten Ordners enthält die Job-ID und den ausgewählten Jobtyp.

In großen Konfigurationen sollten Sie für eine optimale Leistung die Protokolleinstellungen für SnapCenter mithilfe des PowerShell-Cmdlets auf ein minimales Niveau setzen.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10  
-JobLogsMaxFileSize 10MB -Server
```



Um nach Abschluss eines Failover-Jobs auf Integritäts- oder Konfigurationsinformationen zuzugreifen, führen Sie das Cmdlet aus `Get-SmRepositoryConfig`.

## Entfernen Sie Jobs und Protokolle aus SnapCenter

Sie können Sicherungs-, Wiederherstellungs-, Klon- und Überprüfungsaufträge sowie Protokolle aus SnapCenter entfernen. SnapCenter speichert erfolgreiche und fehlgeschlagene Jobprotokolle auf unbestimmte Zeit, sofern Sie sie nicht entfernen. Möglicherweise möchten Sie sie entfernen, um den Speicher aufzufüllen.

### Über diese Aufgabe

Es dürfen derzeit keine Jobs ausgeführt werden. Sie können einen bestimmten Job entfernen, indem Sie eine Job-ID angeben, oder Sie können Jobs innerhalb eines bestimmten Zeitraums entfernen.

Sie müssen den Host nicht in den Wartungsmodus versetzen, um Jobs zu entfernen.

### Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung Folgendes ein: `Open-SMConnection`
3. Geben Sie in der Eingabeaufforderung Folgendes ein: `Remove-SmJobs`
4. Klicken Sie im linken Navigationsbereich auf **Monitor**.
5. Klicken Sie auf der Seite „Überwachen“ auf **Jobs**.
6. Überprüfen Sie auf der Seite „Jobs“ den Status des Jobs.

### Ähnliche Informationen

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"](#).

## Übersicht über die Berichtsfunktionen von SnapCenter

SnapCenter bietet eine Vielzahl von Berichtsoptionen, mit denen Sie die Integrität und den Betriebserfolg Ihres Systems überwachen und verwalten können.

| Berichtstyp               | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sicherungsbericht         | <p>Der Sicherungsbericht bietet allgemeine Daten zu Sicherungstrends für Ihre SnapCenter -Umgebung, zur Erfolgsrate der Sicherung und einige Informationen zu jeder Sicherung, die während des angegebenen Zeitraums durchgeführt wurde. Wenn ein Backup gelöscht wird, zeigt der Bericht keine Statusinformationen zum gelöschten Backup an. Der Sicherungsdetailbericht bietet ausführliche Informationen zu einem angegebenen Sicherungsauftrag und listet die erfolgreich gesicherten Ressourcen sowie alle Ressourcen auf, bei denen ein Backup fehlgeschlagen ist.</p> |
| Klonbericht               | <p>Der Klonbericht bietet allgemeine Daten zu Klontrends für Ihre SnapCenter -Umgebung, zur Klonerfolgsrate und einige Informationen zu jedem Klonauftrag, der während der angegebenen Zeit ausgeführt wurde. Wenn ein Klon gelöscht wird, zeigt der Bericht keine Statusinformationen zum gelöschten Klon an. Der Klondetailbericht enthält Details zum angegebenen Klon, Klonhost und Status der Klonauftragsaufgabe. Wenn eine Aufgabe fehlschlägt, werden im Klondetailbericht Informationen zum Fehler angezeigt.</p>                                                   |
| Wiederherstellungsbericht | <p>Der Wiederherstellungsbericht bietet allgemeine Informationen zu Wiederherstellungsaufträgen. Der Wiederherstellungsdetailbericht enthält Einzelheiten zu einem angegebenen Wiederherstellungsjob, einschließlich Hostname, Sicherungsname, Jobstart und -dauer sowie den Status einzelner Jobaufgaben. Wenn eine Aufgabe fehlschlägt, werden im Wiederherstellungsdetailbericht Informationen zum Fehler angezeigt.</p>                                                                                                                                                  |
| Schutzbericht             | <p>Diese Berichte enthalten Schutzdetails für Ressourcen, die von allen SnapCenter Plug-In-Instanzen verwaltet werden. Dieser Bericht enthält Schutzdetails für Ressourcen, die von allen Plug-in-Instanzen verwaltet werden. Sie können eine Übersicht, Details zu ungeschützten Ressourcen, Ressourcen, die zum Zeitpunkt der Berichterstellung nicht gesichert wurden, Ressourcen einer Ressourcengruppe, für die Sicherungsvorgänge fehlgeschlagen sind, und den SnapVault -Status anzeigen.</p>                                                                         |

| Berichtstyp       | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Geplanter Bericht | <p>Die Ausführung dieser Berichte ist in regelmäßigen Abständen geplant, beispielsweise täglich, wöchentlich oder monatlich. Die Berichte werden automatisch zum angegebenen Datum und zur angegebenen Uhrzeit erstellt und per E-Mail an die entsprechenden Personen gesendet. Sie können die Zeitpläne aktivieren, deaktivieren, ändern oder löschen. Der aktivierte Zeitplan kann bei Bedarf durch Klicken auf die Schaltfläche <b>Jetzt ausführen</b> ausgeführt werden. Der Administrator kann jeden Zeitplan ausführen, der generierte Bericht enthält jedoch Daten basierend auf der Berechtigung des Benutzers, der den Zeitplan erstellt hat.</p> <p>Jeder andere Benutzer außer dem Administrator kann den Zeitplan basierend auf seiner Berechtigung sehen oder ändern. Wenn auf der Seite „Rolle hinzufügen“ die Option „Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen“ ausgewählt ist, können andere Mitglieder dieser Rolle den Zeitplan sehen und ändern.</p> |

## Zugriffsberichte

Mit dem SnapCenter -Dashboard können Sie sich schnell einen Überblick über den Zustand Ihres Systems verschaffen. Vom Dashboard aus können Sie weitere Details einsehen. Alternativ können Sie direkt auf die ausführlichen Berichte zugreifen.

Sie können auf Berichte mit einer der folgenden Methoden zugreifen:

- Klicken Sie im linken Navigationsbereich auf **Dashboard** und dann auf das Kreisdiagramm **Zusammenfassung des letzten Schutzes**, um auf der Seite „Berichte“ weitere Details anzuzeigen.
- Klicken Sie im linken Navigationsbereich auf **Berichte**.

## Filtern Sie Ihren Bericht

Möglicherweise möchten Sie Ihre Berichtsdaten nach einer Reihe von Parametern filtern, je nach Detaillierungsgrad und Zeitraum der von Ihnen benötigten Informationen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte**.
2. Wenn die Parameteransicht nicht angezeigt wird, klicken Sie in der Berichtssymbolleiste auf das Symbol **Parameterbereich umschalten**.
3. Geben Sie den Zeitraum an, für den Sie Ihren Bericht ausführen möchten. + Wenn Sie das Enddatum weglassen, rufen Sie alle verfügbaren Informationen ab.
4. Filtern Sie Ihre Berichtsinformationen anhand der folgenden Kriterien:
  - Ressourcengruppe

- Gastgeber
- Politik
- Ressource
- Status
- Plug-in-Name

5. Klicken Sie auf **Übernehmen**.

## Berichte exportieren oder drucken

Durch das Exportieren von SnapCenter -Berichten können Sie den Bericht in einer Vielzahl alternativer Formate anzeigen. Sie können auch Berichte ausdrucken.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte**.
2. Führen Sie in der Berichtssymbolleiste einen der folgenden Schritte aus:
  - Klicken Sie auf das Symbol **Druckvorschau umschalten**, um eine Vorschau eines druckbaren Berichts anzuzeigen.
  - Wählen Sie ein Format aus der Dropdown-Liste des Symbols **Exportieren** aus, um einen Bericht in ein anderes Format zu exportieren.
3. Um einen Bericht zu drucken, klicken Sie auf das Symbol **Drucken**.
4. Um eine bestimmte Berichtszusammenfassung anzuzeigen, scrollen Sie zum entsprechenden Abschnitt des Berichts.

## SMTP-Server für E-Mail-Benachrichtigungen festlegen

Sie können den SMTP-Server angeben, der zum Senden von Datenschutz-Jobberichten an Sie selbst oder an andere verwendet werden soll. Sie können auch eine Test-E-Mail senden, um die Konfiguration zu überprüfen. Die Einstellungen werden global für jeden SnapCenter -Job angewendet, für den Sie eine E-Mail-Benachrichtigung konfigurieren.

Diese Option konfiguriert den SMTP-Server zum Senden aller Datenschutz-Jobberichte. Wenn Sie jedoch regelmäßige SnapCenter Datenschutzjob-Updates für eine bestimmte Ressource an sich selbst oder an andere senden möchten, damit Sie den Status dieser Updates überwachen können, können Sie beim Erstellen einer Ressourcengruppe die Option zum E-Mail-Versand der SnapCenter -Berichte konfigurieren.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Geben Sie den SMTP-Server ein und klicken Sie auf **Speichern**.
4. Um eine Test-E-Mail zu senden, geben Sie die E-Mail-Adresse ein, von der und an die Sie die E-Mail senden möchten, geben Sie den Betreff ein und klicken Sie auf **Senden**.

## Konfigurieren Sie die Option zum Versenden von Berichten per E-Mail

Wenn Sie regelmäßige Updates zu SnapCenter -Datenschutzaufträgen an sich selbst oder andere senden lassen möchten, damit Sie den Status dieser Updates überwachen können, können Sie beim Erstellen einer

Ressourcengruppe die Option zum E-Mail-Versand der SnapCenter -Berichte konfigurieren.

### Bevor Sie beginnen

Sie müssen Ihren SMTP-Server auf der Seite „Globale Einstellungen“ unter „Einstellungen“ konfiguriert haben.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie den Ressourcentyp aus, den Sie anzeigen möchten, und klicken Sie auf **Neue Ressourcengruppe**, oder wählen Sie eine vorhandene Ressourcengruppe aus und klicken Sie auf **Ändern**, um E-Mail-Berichte für eine vorhandene Ressourcengruppe zu konfigurieren.
3. Wählen Sie im Benachrichtigungsbereich des Assistenten „Neue Ressourcengruppe“ aus dem Pulldown-Menü aus, ob Sie immer, bei Fehlern oder bei Fehlern oder Warnungen Berichte erhalten möchten.
4. Geben Sie die Adresse ein, von der die E-Mail gesendet wird, die Adresse, an die die E-Mail gesendet wird, und den Betreff der E-Mail.

## Verwalten des SnapCenter Server-Repository

Informationen zu verschiedenen von SnapCenter ausgeführten Vorgängen werden im Datenbank-Repository des SnapCenter Servers gespeichert. Sie müssen Backups des Repositories erstellen, um den SnapCenter -Server vor Datenverlust zu schützen.

Das SnapCenter Server-Repository wird manchmal als NSM-Datenbank bezeichnet.

### Voraussetzungen zum Schutz des SnapCenter -Repositorys

Ihre Umgebung sollte bestimmte Voraussetzungen erfüllen, um das SnapCenter Repository zu schützen.

- Verwalten von Verbindungen virtueller Speichermaschinen (SVM)

Sie sollten die Speicheranmeldeinformationen konfigurieren.

- Bereitstellen von Hosts

Auf dem SnapCenter -Repository-Host sollte mindestens eine NetApp Speicherfestplatte vorhanden sein. Wenn auf dem SnapCenter -Repository-Host keine NetApp Festplatte vorhanden ist, müssen Sie eine erstellen.

Einzelheiten zum Hinzufügen von Hosts, Einrichten von SVM-Verbindungen und Bereitstellen von Hosts finden Sie in den Installationsanweisungen.

- Bereitstellung von iSCSI LUN oder VMDK

Für eine Hochverfügbarkeitskonfiguration (HA) können Sie entweder ein iSCSI-LUN oder ein VMDK auf einem der SnapCenter -Server bereitstellen.

### Sichern Sie das SnapCenter Repository

Durch die Sicherung des SnapCenter Server-Repositorys können Sie es vor Datenverlust schützen. Sie können das Repository sichern, indem Sie das Cmdlet *Protect-SmRepository* ausführen.

## Über diese Aufgabe

Das Cmdlet *Protect-SmRepository* führt die folgenden Aufgaben aus:

- Erstellt eine Ressourcengruppe und eine Richtlinie
- Erstellt einen Sicherungszeitplan für das SnapCenter -Repository

### Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Sichern Sie das Repository mit dem Cmdlet *Protect-SmRepository* und den erforderlichen Parametern.

## Anzeigen von Backups des SnapCenter -Repositorys

Sie können eine Liste der Datenbank-Repository-Sicherungen des SnapCenter Servers anzeigen, indem Sie das Cmdlet *Get-SmRepositoryBackups* ausführen.

Die Repository-Sicherungen werden gemäß dem im Cmdlet *Protect-SmRepository* angegebenen Zeitplan erstellt.

### Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung das folgende Cmdlet ein und geben Sie dann die Anmeldeinformationen für die Verbindung mit dem SnapCenter -Server ein: *Open-SMConnection*
3. Listen Sie alle verfügbaren SnapCenter -Datenbanksicherungen mit dem Cmdlet *Get-SmRepositoryBackups* auf.

## Wiederherstellen des SnapCenter -Datenbankrepositorys

Sie können das SnapCenter Repository wiederherstellen, indem Sie das Cmdlet *Restore-SmRepositoryBackup* ausführen.

Wenn Sie das SnapCenter -Repository wiederherstellen, werden andere laufende SnapCenter Vorgänge beeinträchtigt, da während des Wiederherstellungsvorgangs nicht auf die Repository-Datenbank zugegriffen werden kann.

### Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung das folgende Cmdlet ein und geben Sie dann die Anmeldeinformationen für die Verbindung mit dem SnapCenter -Server ein: *Open-SMConnection*
3. Stellen Sie die Repository-Sicherung mit dem Cmdlet *Restore-SmRepositoryBackup* wieder her.

Das folgende Cmdlet stellt das SnapCenter MySQL-Datenbank-Repository aus den auf iSCSI LUN oder VMDK vorhandenen Sicherungen wieder her:



```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-  
x3550-s09_09-15-2016_10.32.00.4445
```

Das folgende Cmdlet stellt die SnapCenter MySQL-Datenbank wieder her, wenn Sicherungsdateien versehentlich im iSCSI-LUN gelöscht werden. Stellen Sie für VMDK das Backup manuell aus ONTAP -Snapshots wieder her.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-  
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```



Die Sicherung, die zum Ausführen des Repository-Wiederherstellungsvorgangs verwendet wurde, wird nicht aufgelistet, wenn die Repository-Sicherungen nach dem Ausführen des Wiederherstellungsvorgangs abgerufen werden.

## Migrieren des SnapCenter -Repositorys

Sie können das Datenbank-Repository des SnapCenter Servers vom Standardspeicherort auf eine andere Festplatte migrieren. Sie können das Repository migrieren, wenn Sie es auf eine Festplatte mit mehr Speicherplatz verschieben möchten.

### Schritte

1. Stoppen Sie den MYSQL57-Dienst in Windows.
2. Suchen Sie das MySQL-Datenverzeichnis.

Normalerweise finden Sie das Datenverzeichnis unter C:\ProgramData\MySQL\MySQL Server 5.7\Data.

3. Kopieren Sie das MySQL-Datenverzeichnis an den neuen Speicherort, beispielsweise E:\Data\msm.
4. Klicken Sie mit der rechten Maustaste auf das neue Verzeichnis und wählen Sie dann **Eigenschaften > Sicherheit**, um das lokale Serverkonto des Netzwerkdienstes zum neuen Verzeichnis hinzuzufügen und dem Konto dann Vollzugriff zuzuweisen.
5. Benennen Sie das ursprüngliche Datenbankverzeichnis um, beispielsweise in msm\_copy.
6. Erstellen Sie in einer Windows-Eingabeaufforderung mit dem Befehl *mklink* einen symbolischen Verzeichnislink.

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\msm" "E:\Data\msm" "
```

7. Starten Sie den MYSQL57-Dienst in Windows.
8. Überprüfen Sie, ob die Änderung des Datenbankspeicherorts erfolgreich war, indem Sie sich bei SnapCenter anmelden und die Repository-Einträge überprüfen oder indem Sie sich beim MySQL-Dienstprogramm anmelden und eine Verbindung zum neuen Repository herstellen.
9. Löschen Sie das ursprüngliche, umbenannte Datenbank-Repository-Verzeichnis (msm\_copy).

## Setzen Sie das Kennwort für das SnapCenter -Repository zurück

Das Datenbankkennwort für das MySQL-Server-Repository wird während der SnapCenter -Serverinstallation

von SnapCenter 4.2 automatisch generiert. Dieses automatisch generierte Passwort ist dem SnapCenter -Benutzer zu keinem Zeitpunkt bekannt. Wenn Sie auf die Repository-Datenbank zugreifen möchten, sollten Sie das Passwort zurücksetzen.

### Bevor Sie beginnen

Sie sollten über die Administratorrechte von SnapCenter verfügen, um das Kennwort zurückzusetzen.

### Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein und geben Sie dann die Anmeldeinformationen für die Verbindung mit dem SnapCenter -Server ein: *Open-SMConnection*
3. Setzen Sie das Repository-Passwort zurück: *Set-SmRepositoryPassword*

Der folgende Befehl setzt das Repository-Passwort zurück:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: *****
ConfirmPassword: *****
Successfully updated the MySQL server password.
```

### Ähnliche Informationen

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"](#) .

## Verwalten von Ressourcen nicht vertrauenswürdiger Domänen

SnapCenter verwaltet nicht nur Hosts in vertrauenswürdigen Active Directory-Domänen (AD), sondern auch Hosts in mehreren nicht vertrauenswürdigen AD-Domänen. Die nicht vertrauenswürdigen AD-Domänen müssen beim SnapCenter -Server registriert werden. SnapCenter unterstützt Benutzer und Gruppen mehrerer nicht vertrauenswürdiger AD-Domänen.

Sie können den SnapCenter -Server auf einem Computer installieren, der sich entweder in einer Domäne oder einer Arbeitsgruppe befindet. Um den SnapCenter -Server zu installieren, sollten Sie die Domänenanmeldeinformationen angeben, wenn sich der Computer in einer Domäne befindet, oder die lokalen Administratoranmeldeinformationen, wenn sich der Computer in einer Arbeitsgruppe befindet.

Active Directory (AD)-Gruppen, die zu Domänen gehören, die nicht beim SnapCenter -Server registriert sind, werden nicht unterstützt. Obwohl Sie mit diesen AD-Gruppen SnapCenter -Rollen erstellen können, schlägt die Anmeldung beim SnapCenter Server mit der folgenden Fehlermeldung fehl: Der Benutzer, bei dem Sie sich anmelden möchten, gehört keiner Rolle an. Bitte wenden Sie sich an den Administrator.

## Ändern nicht vertrauenswürdiger Domänen

Sie können eine nicht vertrauenswürdige Domäne ändern, wenn Sie die IP-Adressen des Domänencontrollers oder den vollqualifizierten Domänennamen (FQDN) aktualisieren möchten.

### Über diese Aufgabe

Nachdem Sie den FQDN geändert haben, funktionieren die zugehörigen Assets (Hosts, Benutzer und Gruppen) möglicherweise nicht wie erwartet.

Um eine nicht vertrauenswürdige Domäne zu ändern, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell-Cmdlets verwenden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Klicken Sie auf der Seite „Globale Einstellungen“ auf **Domäneneinstellungen**.

4.  und geben Sie dann die folgenden Details an:

| Für dieses Feld...                 | Machen Sie Folgendes...                                                                                               |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Domänen-FQDN                       | Geben Sie den FQDN an und klicken Sie auf <b>Auflösen</b> .                                                           |
| IP-Adressen des Domänencontrollers | Wenn der Domänen-FQDN nicht aufgelöst werden kann, geben Sie eine oder mehrere IP-Adressen des Domänencontrollers an. |

5. Klicken Sie auf **OK**.

## Aufheben der Registrierung nicht vertrauenswürdiger Active Directory-Domänen

Sie können die Registrierung einer nicht vertrauenswürdigen Active Directory-Domäne aufheben, wenn Sie die mit dieser Domäne verknüpften Assets nicht verwenden möchten.

### Bevor Sie beginnen

Sie sollten die Hosts, Benutzer, Gruppen und Anmeldeinformationen entfernt haben, die mit der nicht vertrauenswürdigen Domäne verknüpft sind.

### Über diese Aufgabe

- Nachdem die Domäne vom SnapCenter -Server abgemeldet wurde, können Benutzer dieser Domäne nicht mehr auf den SnapCenter -Server zugreifen.
- Wenn zugehörige Assets (Hosts, Benutzer und Gruppen) vorhanden sind, sind diese Assets nach der Abmeldung der Domäne nicht mehr betriebsbereit.
- Um die Registrierung einer nicht vertrauenswürdigen Domäne aufzuheben, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell-Cmdlets verwenden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Klicken Sie auf der Seite „Globale Einstellungen“ auf **Domäneneinstellungen**.
4. Wählen Sie aus der Domänenliste die Domäne aus, deren Registrierung Sie aufheben möchten.
5. Klicken  und klicken Sie dann auf **OK**.

## Verwalten des Speichersystems

Nachdem Sie das Speichersystem hinzugefügt haben, können Sie die Konfiguration und Verbindungen des Speichersystems ändern oder das Speichersystem löschen.

### Ändern der Speichersystemkonfiguration

Sie können SnapCenter verwenden, um die Konfiguration Ihres Speichersystems zu ändern, wenn Sie den Benutzernamen, das Kennwort, die Plattform, den Port, das Protokoll, die Zeitüberschreitungsdauer, die bevorzugte IP-Adresse oder die Nachrichtenoptionen ändern möchten.

### Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe ändern. Wenn Sie zu einer oder mehreren Gruppen mit Berechtigung für dasselbe Speichersystem gehören, wird der Name der Speicherverbindung in der Speicherverbindungsliste mehrmals angezeigt, einmal für jede Gruppe mit Berechtigung für das Speichersystem.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Führen Sie auf der Seite „Speichersysteme“ im Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

| Wählen...  | Schritte...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP SVMs | <p data-bbox="842 159 1438 258">Um alle hinzugefügten virtuellen Speichermaschinen (SVMs) anzuzeigen und die erforderliche SVM-Konfiguration zu ändern.</p> <ol data-bbox="854 296 1468 968" style="list-style-type: none"> <li data-bbox="854 296 1289 394">a. Klicken Sie auf der Seite „Speicherverbindungen“ auf den entsprechenden SVM-Namen.</li> <li data-bbox="854 415 1468 968">b. Führen Sie eine der folgenden Aktionen aus: <ul style="list-style-type: none"> <li data-bbox="915 478 1468 678">◦ Wenn die SVM nicht Teil eines Clusters ist, ändern Sie auf der Seite „Speichersystem ändern“ die Konfigurationen wie Benutzername, Kennwort, EMS- und AutoSupport -Einstellungen, Plattform, Protokoll, Port, Timeout und bevorzugte IP.</li> <li data-bbox="915 699 1468 968">◦ Wenn die SVM Teil eines Clusters ist, wählen Sie auf der Seite „Speichersystem ändern“ die Option „SVM unabhängig verwalten“ und ändern Sie die Konfigurationen wie Benutzername, Kennwort, EMS- und AutoSupport -Einstellungen, Plattform, Protokoll, Port, Timeout und bevorzugte IP.</li> </ul> </li> </ol> <p data-bbox="938 1003 1474 1203">Wenn Sie sich nach der Änderung der SVM für eine unabhängige Verwaltung für die Verwaltung über einen Cluster entscheiden, sollten Sie die SVM löschen und dann auf „Neu erkennen“ klicken. Die SVM wird dem ONTAP Cluster hinzugefügt.</p> <div data-bbox="922 1255 1446 1696">  <p data-bbox="1036 1255 1446 1696">Wenn ein Speichersystemkennwort auf der SnapCenter -GUI aktualisiert wird, sollten Sie die SMCore-Dienste des jeweiligen Plug-Ins oder des Serverhosts neu starten, da das aktualisierte Kennwort nicht in SMCore angezeigt wird und die Sicherungsaufträge mit einem Fehler bezüglich falscher Anmeldeinformationen fehlschlagen.</p> </div> |

| Wählen...     | Schritte...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP Cluster | <p>Um alle hinzugefügten Cluster anzuzeigen und die erforderliche Clusterkonfiguration zu ändern.</p> <ol style="list-style-type: none"> <li>Klicken Sie auf der Seite „Speicherverbindungen“ auf den Clusternamen.</li> <li>Klicken Sie auf der Seite „Speichersystem ändern“ auf das Bearbeitungssymbol neben „Benutzername“ und ändern Sie den Benutzernamen und das Kennwort.</li> <li>Wählen oder löschen Sie die EMS- und AutoSupport -Einstellungen.</li> <li>Klicken Sie auf <b>Weitere Optionen</b> und ändern Sie andere Konfigurationen wie Plattform, Protokoll, Port, Timeout und bevorzugte IP.</li> </ol> |

3. Klicken Sie auf **Senden**.

## Löschen Sie das Speichersystem

Mit SnapCenter können Sie alle nicht verwendeten Speichersysteme löschen.

### Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe löschen. Wenn Sie zu einer oder mehreren Gruppen mit Berechtigung für dasselbe Speichersystem gehören, wird der Name des Speichersystems in der Speicherverbindungsliste mehrmals angezeigt, einmal für jede Gruppe mit Berechtigung für das Speichersystem.



Wenn Sie ein Speichersystem löschen, schlagen alle auf diesem Speichersystem ausgeführten Vorgänge fehl.

### Schritte

- Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
- Wählen Sie auf der Seite „Speichersysteme“ aus der Dropdown-Liste **Typ** entweder \* ONTAP SVMs\* oder \* ONTAP Clusters\* aus.
- Aktivieren Sie auf der Seite „Speicherverbindungen“ entweder das Kontrollkästchen neben der SVM oder dem Cluster, den Sie löschen möchten.



Sie können die SVM, die Teil eines Clusters ist, nicht auswählen.

- Klicken Sie auf **Löschen**.
- Klicken Sie auf der Seite „Verbindungseinstellungen des Speichersystems löschen“ auf **OK**.



Wenn ein SVM mithilfe der ONTAP -GUI aus dem ONTAP Cluster gelöscht wird, klicken Sie in der SnapCenter -GUI auf **Neu erkennen**, um die SVM-Liste zu aktualisieren.

## REST-API-Unterstützung

Alle ASA, AFF oder FAS -Systemverbindungen zu ONTAP erfolgen standardmäßig über ZAPI. REST API kann für bestimmte ONTAP Versionen aktiviert werden.

SnapCenter nutzt REST-APIs, um alle Vorgänge auf ASA r2-Systemen auszuführen, die ZAPIs nicht unterstützen.

Sie können die Konfigurationsschlüssel in den folgenden Konfigurationsdateien ändern:

- IsRestEnabledForStorageConnection

Der Standardwert ist „false“.

- MinOntapVersionToUseREST

Der Standardwert ist 9.13.1.

### Verbindung über REST-API aktivieren

1. Setzen Sie IsRestEnabledForStorageConnection auf „true“.
2. Fügen Sie den Schlüssel in SMCoreServiceHost.dll.config und SnapDriveService.dll.config sowohl auf dem Server als auch auf den Windows-Plug-In-Hosts hinzu.

```
<add key="IsRestEnabledForStorageConnection" value="true" />
```

### Beschränken Sie die Verbindung über die REST-API auf eine bestimmte ONTAP Version.

1. Setzen Sie den Konfigurationsparameter MinOntapVersionToUseREST auf „true“.
2. Fügen Sie den Schlüssel in SMCoreServiceHost.dll.config und SnapDriveService.dll.config sowohl auf dem Server als auch auf den Windows-Plug-In-Hosts hinzu.

```
<add key="MinOntapVersionToUseREST" value="9.13.1" />
```

3. Starten Sie den Dienst für SmCore auf dem Server und den Plug-In- und SnapDrive -Dienst auf der Plug-In-Maschine neu.

## Verwalten der EMS-Datenerfassung

Sie können die Datenerfassung des Event Management System (EMS) mithilfe von PowerShell-Cmdlets planen und verwalten. Bei der EMS-Datenerfassung werden Details zum SnapCenter -Server, den installierten SnapCenter Plug-In-Paketen, den Hosts und ähnlichen Informationen gesammelt und anschließend an eine angegebene ONTAP Storage Virtual Machine (SVM) gesendet.



Die CPU-Auslastung des Systems ist hoch, wenn eine Datenerfassungsaufgabe ausgeführt wird. Die CPU-Auslastung bleibt hoch, solange der Vorgang ausgeführt wird, unabhängig von der Datengröße.

### Stoppen Sie die EMS-Datenerfassung

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird alle sieben Tage nach Ihrem Installationsdatum

ausgeführt. Sie können die Datenerfassung jederzeit mithilfe des PowerShell-Cmdlets *Disable-SmDataCollectionEMS* deaktivieren.

#### Schritte

1. Stellen Sie über eine PowerShell-Befehlszeile eine Sitzung mit SnapCenter her, indem Sie *Open-SmConnection* eingeben.
2. Deaktivieren Sie die EMS-Datenerfassung, indem Sie *Disable-SmDataCollectionEms* eingeben.

## Starten Sie die EMS-Datenerfassung

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird ab dem Installationsdatum alle sieben Tage ausgeführt. Wenn Sie es deaktiviert haben, können Sie die EMS-Datenerfassung mithilfe des Cmdlets *Enable-SmDataCollectionEMS* erneut starten.

Dem Benutzer der Storage Virtual Machine (SVM) wurde die Berechtigung „Generate-Autosupport-Log“ für das NetApp ONTAP Ereignis erteilt.

#### Schritte

1. Stellen Sie über eine PowerShell-Befehlszeile eine Sitzung mit SnapCenter her, indem Sie *Open-SmConnection* eingeben.
2. Aktivieren Sie die EMS-Datenerfassung, indem Sie *Enable-SmDataCollectionEMS* eingeben.

## Ändern Sie den Zeitplan für die EMS-Datenerfassung und das Ziel-SVM

Sie können PowerShell-Cmdlets verwenden, um den Zeitplan für die EMS-Datenerfassung oder die Ziel-Storage-Virtual-Machine (SVM) zu ändern.

#### Schritte

1. Um eine Sitzung mit SnapCenter herzustellen, geben Sie in einer PowerShell-Befehlszeile das Cmdlet *Open-SmConnection* ein.
2. Um das EMS-Datenerfassungsziel zu ändern, geben Sie das Cmdlet *Set-SmDataCollectionEmsTarget* ein.
3. Um den Zeitplan für die EMS-Datenerfassung zu ändern, geben Sie das Cmdlet *Set-SmDataCollectionEmsSchedule* ein.

## Überwachen Sie den Status der EMS-Datenerfassung

Sie können den Status Ihrer EMS-Datenerfassung mithilfe mehrerer PowerShell-Cmdlets überwachen. Sie können Informationen zum Zeitplan, zum Ziel der Storage Virtual Machine (SVM) und zum Status abrufen.

#### Schritte

1. Stellen Sie über eine PowerShell-Befehlszeile eine Sitzung mit SnapCenter her, indem Sie *Open-SmConnection* eingeben.
2. Rufen Sie Informationen zum EMS-Datenerfassungszeitplan ab, indem Sie *Get-SmDataCollectionEmsSchedule* eingeben.
3. Rufen Sie Informationen zum Status der EMS-Datenerfassung ab, indem Sie *Get-SmDataCollectionEmsStatus* eingeben.
4. Rufen Sie Informationen zum EMS-Datenerfassungsziel ab, indem Sie *Get-SmDataCollectionEmsTarget* eingeben.

## Ähnliche Informationen



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"](#) .

# Aktualisieren Sie SnapCenter Server und Plug-Ins

## Konfigurieren Sie SnapCenter , um nach verfügbaren Updates zu suchen

SnapCenter kommuniziert regelmäßig mit der NetApp -Support-Site, um Sie über verfügbare Software-Updates zu informieren. Sie können auch einen Zeitplan erstellen, um das Intervall festzulegen, in dem Sie Informationen zu verfügbaren Updates erhalten möchten.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf **Software**.

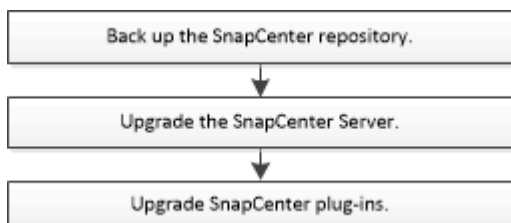
Auf der Seite „Verfügbare Software“ werden die verfügbaren Plug-In-Pakete, die verfügbaren Versionen und deren Installationsstatus angezeigt.

3. Klicken Sie auf **Nach Updates suchen**, um zu sehen, ob neuere Versionen von Plug-in-Paketen verfügbar sind.
4. Klicken Sie auf **Updates planen**, um einen Zeitplan zu erstellen und das Intervall festzulegen, in dem Sie Informationen zu verfügbaren Updates erhalten möchten:
  - a. Wählen Sie das Intervall unter **Nach Updates suchen**.
  - b. Wählen Sie die Windows-Anmeldeinformationen des SnapCenter Server-Administrators aus und klicken Sie auf **OK**.

## Upgrade-Workflow

Jede Version von SnapCenter enthält ein aktualisiertes SnapCenter -Server- und Plug-in-Paket. Plug-in-Paket-Updates werden mit dem SnapCenter -Installationsprogramm verteilt. Sie können SnapCenter so konfigurieren, dass nach verfügbaren Updates gesucht wird.

Der Workflow zeigt die verschiedenen Aufgaben, die zum Upgrade des SnapCenter -Servers und der Plug-in-Pakete erforderlich sind.



## Unterstützte Upgradepfade

Der Upgradepfad hilft Ihnen zu verstehen, von welchen früheren Versionen von SnapCenter Sie auf die neuesten Versionen von SnapCenter aktualisieren können und welche Versionen der Plug-Ins unterstützt

werden.

| Wenn Sie die SnapCenter Server-Version verwenden ... | Sie können SnapCenter Server direkt aktualisieren auf... | Unterstützte Plug-in-Versionen |
|------------------------------------------------------|----------------------------------------------------------|--------------------------------|
| 5,0                                                  | 6,0                                                      | • 5,0<br>• 6,0                 |
|                                                      | 6.0.1                                                    | • 6.0.1                        |
|                                                      | 6,1                                                      | • 6,1                          |
| 6,0                                                  | 6.0.1                                                    | • 6,0<br>• 6.0.1               |
|                                                      | 6,1                                                      | • 6,1                          |
| 6.0.1                                                | 6,1                                                      | • 6.0.1<br>• 6,1               |

Informationen zum Upgrade des SnapCenter Plug-in for VMware vSphere finden Sie unter ["Aktualisieren Sie das SnapCenter Plug-in for VMware vSphere"](#) .

## Aktualisieren Sie den SnapCenter -Server auf dem Windows-Host

Sie sollten den SnapCenter -Server aktualisieren, um auf die neuesten Funktionen und Verbesserungen der neuesten Version zugreifen zu können.

### Bevor Sie beginnen

- Aktualisieren Sie den SnapCenter Server-Host mit den neuesten Windows-Updates und stellen Sie sicher, dass keine Systemneustarts ausstehen.
- Stellen Sie sicher, dass keine anderen Vorgänge ausgeführt werden, bevor Sie mit dem Upgrade beginnen.
- Installieren Sie ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting Bundle und PowerShell 7.4.2 oder höher.
- Sichern Sie die SnapCenter -Repository-Datenbank (MySQL), nachdem Sie sichergestellt haben, dass keine Jobs ausgeführt werden. Dies wird vor dem Upgrade von SnapCenter Server und dem Exchange-Plug-In empfohlen.

Weitere Informationen finden Sie unter ["Sichern Sie das SnapCenter Repository"](#) .

- Sichern Sie alle geänderten SnapCenter -Konfigurationsdateien, die Sie entweder auf dem SnapCenter Server-Host oder dem Plug-In-Host geändert haben.

Beispiele für SnapCenter -Konfigurationsdateien: SnapDriveService.exe.config, SMCOREServiceHost.exe.config usw.

- Wenn Sie mehrere Versionen des benutzerdefinierten Plug-Ins in SnapCenter 5.0 installiert haben, sollten Sie vor dem Upgrade auf 6.0 oder höher die Powershell-Cmdlets ausführen, um alle früheren Versionen des benutzerdefinierten Plug-Ins (mit Ausnahme der neuesten) aus dem SnapCenter Repository (NSM-Datenbank) zu entfernen.
  - Laufen `Open-SmConnection` und melden Sie sich mit den Anmeldeinformationen der `SnapCenterAdmin`-Rolle an
  - Laufen `Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>`

Weitere Informationen finden Sie unter "[Das Upgrade auf SnapCenter 6.0 oder höher schlägt fehl](#)".

### Informationen zu diesem Vorgang

- Während des Upgrades führt SnapCenter ein SQL-Skript aus, um die Exchange-Daten in der NSM-Datenbank zu aktualisieren und den DAG- und Host-Kurznamen in FQDN umzuwandeln. Dies gilt nur, wenn Sie SnapCenter Server mit dem Exchange-Plug-In verwenden.
- Wenn Sie den Serverhost manuell in den Wartungsmodus versetzt haben, wählen Sie nach dem Upgrade **Hosts > Zeitplan aktivieren**, um den Serverhost aus dem Wartungsmodus zu holen.
- Für die vorhandenen Sicherungs- und Überprüfungszeitpläne mit in der Richtlinie aktivierten Prescripts und Postscripts funktionieren die Sicherungsvorgänge nach dem Upgrade weiterhin.

Auf der Seite **Auftragsdetails** wird in einer Warnmeldung empfohlen, dass der Kunde die Skripte in den `SCRIPTS_PATH` kopieren und die Richtlinie bearbeiten sollte, um einen Pfad bereitzustellen, der relativ zum `SCRIPTS_PATH` ist. Beim Klon-Lebenszyklusjob wird die Warnmeldung auf der Ebene des Unterjobs angezeigt.

### Schritte

1. Laden Sie das SnapCenter Server-Installationspaket von der NetApp Support-Site herunter.

<https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab>

2. Erstellen Sie eine Kopie der Datei `web.config` unter `C:\Programme\NetApp\SnapCenter WebApp`.
3. Exportieren Sie die Host-Zeitpläne des SnapCenter -Plug-Ins aus dem Windows-Taskplaner, um sie wiederherzustellen, falls das Upgrade fehlschlägt.

```
md d:\\SCBackup`\\schtasks /query /xml /TN taskname >>
"D:\\SCBackup\\taskname.xml"
```

4. Erstellen Sie den SnapCenter MySQL-Datenbank-Dump, wenn die Repository-Sicherung nicht konfiguriert ist.

```
md d:\\SCBackup`\\mysqldump --all-databases --single-transaction --add-drop
-database --triggers --routines --events -u root -p >
D:\\SCBackup\\SCRepoBackup.dmp
```

Geben Sie bei der entsprechenden Aufforderung das Kennwort ein.

5. Doppelklicken Sie auf die heruntergeladene EXE-Datei, um das SnapCenter Server-Upgrade zu starten.

Nachdem Sie das Upgrade gestartet haben, führt SnapCenter Vorprüfungen durch. Wenn das System die Mindestanforderungen nicht erfüllt, zeigt SnapCenter Fehler- oder Warnmeldungen an. Sie können Warnungen ignorieren und mit der Installation fortfahren, müssen jedoch alle Fehler beheben.



SnapCenter verwendet weiterhin das vorhandene Datenbankkennwort des MySQL Server-Repositorys, das bei der Installation der früheren Version von SnapCenter Server bereitgestellt wurde.

## 6. Wählen Sie **Upgrade**.

Wenn Sie zu irgendeinem Zeitpunkt **Abbrechen** auswählen, stoppt SnapCenter das Upgrade. Der SnapCenter -Server wird nicht auf den vorherigen Zustand zurückgesetzt.

**Best Practice:** Melden Sie sich ab und erneut an oder öffnen Sie einen neuen Browser, um auf die SnapCenter Benutzeroberfläche zuzugreifen.

### Nach Abschluss

- Wenn das Plug-In mit einem Sudo-Benutzer installiert wird, sollten Sie die unter *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc\_unix\_plugins\_checksum.txt* verfügbaren SHA224-Schlüssel kopieren, um die Datei */etc/sudoers* zu aktualisieren.
- Sie sollten eine neue Ermittlung der Ressourcen auf dem Serverhost durchführen.

Wenn SnapCenter den Server-Hoststatus als „gestoppt“ anzeigt, warten Sie einige Zeit und führen Sie eine neue Erkennung durch. Sie können den Wert des Parameters **HostRefreshInterval** (Standardwert ist 3600 Sekunden) auch auf einen beliebigen Wert über 10 Minuten ändern.

- Wenn das Upgrade fehlschlägt, bereinigen Sie die fehlgeschlagene Installation, installieren Sie die frühere Version von SnapCenter neu und stellen Sie den vorherigen Zustand der NSM-Datenbank wieder her.
- Nach dem Upgrade des Serverhosts müssen Sie auch die Plug-Ins aktualisieren, bevor Sie ein Speichersystem hinzufügen.

## Aktualisieren Sie den SnapCenter -Server auf dem Linux-Host

Sie können die SnapCenter Server-Installationsdatei verwenden, um den SnapCenter Server zu aktualisieren.

### Schritte

1. Führen Sie eine der Aktionen aus, um den SnapCenter -Server zu aktualisieren.

| Wenn Sie auftreten möchten ... | Machen Sie Folgendes...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nicht interaktives Upgrade     | <pre>sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DUPGRADE=&lt;value&gt; -DINSTALL_LOG_NAME=&lt;filename&gt;</pre> <p>Beispiel: <code>sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log</code></p> <p>Protokolle werden unter <i>/var/opt/snapcenter/logs</i> gespeichert.</p> <p>Für das Upgrade zu übergebende Parameter:</p> <ul style="list-style-type: none"> <li>• <b>DINSTALL_LOG_NAME:</b> Name der Protokolldatei, in der die Installationsprotokolle gespeichert werden.</li> <li>• <b>DUPGRADE:</b> Der Standardwert ist 0. Geben Sie diesen Parameter und seinen Wert als eine beliebige Ganzzahl ungleich 0 an, um den SnapCenter -Server zu aktualisieren.</li> </ul> |
| Interaktive Installation       | <pre>./snapcenter-linux-server- (e18/e19/sles15).bin</pre> <p>Sie werden zur Bestätigung des Upgrades aufgefordert. Geben Sie einen beliebigen Wert außer 0 ein, um das SnapCenter Server-Upgrade zu bestätigen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



Sie sollten sich entweder abmelden und dann bei SnapCenter anmelden oder den Browser schließen und dann einen neuen öffnen, um auf die SnapCenter -GUI zuzugreifen.

## Aktualisieren Sie Ihre Plug-in-Pakete

Die Plug-In-Pakete werden als Teil des SnapCenter Upgrades verteilt.

Sie müssen nicht jeden Plug-in-Host, den Sie aktualisieren möchten, manuell in den Wartungsmodus versetzen, da das Aktualisierungsverfahren Ihre Windows-, Linux- oder AIX-Plug-in-Hosts in den Wartungsmodus versetzt. Der Wartungsmodus verhindert, dass während des Upgrades geplante Jobs auf dem Plug-In-Host ausgeführt werden.

### Bevor Sie beginnen

- Wenn Sie kein Root-Benutzer mit Zugriff auf die Linux-Maschinen sind, sollten Sie die Datei */etc/sudoers* mit den neuesten Prüfsummenwerten aktualisieren, bevor Sie den Upgrade-Vorgang durchführen.
- Standardmäßig erkennt SnapCenter **JAVA\_HOME** aus der Umgebung. Wenn Sie ein festes **JAVA\_HOME** verwenden möchten und die Plug-Ins auf einem Linux-Host aktualisieren, sollten Sie den Parameter **SKIP\_JAVAHOME\_UPDATE** manuell in der Datei *spl.properties* unter */var/opt/snapcenter/spl/etc/*

hinzufügen und den Wert auf TRUE setzen.

Der Wert von JAVA\_HOME wird aktualisiert, wenn das Plug-In aktualisiert wird oder wenn der SnapCenter Plug-In Loader (SPL)-Dienst neu gestartet wird. Wenn Sie vor dem Upgrade oder Neustart der SPL den Parameter SKIP\_JAVAHOME\_UPDATE hinzufügen und den Wert auf TRUE setzen, wird der Wert von JAVA\_HOME nicht aktualisiert.

- Sie sollten alle SnapCenter -Konfigurationsdateien gesichert haben, die Sie entweder auf dem SnapCenter Server-Host oder dem Plug-In-Host geändert haben.

Beispiele für SnapCenter -Konfigurationsdateien: SnapDriveService.exe.config, SMCoreserviceHost.exe.config usw.

### Informationen zu diesem Vorgang

- Für das SnapCenter -Plug-in für Microsoft SQL Server, das SnapCenter -Plug-in für Microsoft Exchange Server und das SnapCenter -Plug-in für Microsoft Windows wird empfohlen, sowohl den Server als auch die Plug-in-Hosts auf die neueste Version zu aktualisieren, damit SCRIPTS\_PATH ausgeführt werden kann.

Für die vorhandenen Sicherungs- und Überprüfungszeitpläne mit in der Richtlinie aktivierten Prescripts und Postscripts funktionieren die Sicherungsvorgänge nach dem Upgrade weiterhin.

Auf der Seite **Auftragsdetails** wird in einer Warnmeldung empfohlen, dass der Kunde die Skripte in den SCRIPTS\_PATH kopieren und die Richtlinie bearbeiten sollte, um einen Pfad bereitzustellen, der relativ zum SCRIPTS\_PATH ist. Beim Klon-Lebenszyklusjob wird die Warnmeldung auf der Ebene des Unterjobs angezeigt.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts > Verwaltete Hosts**.
2. Aktualisieren Sie die Hosts, indem Sie eine der folgenden Aufgaben ausführen:
  - Wenn in der Spalte „Gesamtstatus“ für einen der Plug-In-Hosts „Upgrade verfügbar“ angezeigt wird, klicken Sie auf den Namen des Plug-In-Hosts und führen Sie die folgenden Schritte aus:
    - i. Klicken Sie auf **Weitere Optionen**.
    - ii. Wählen Sie **Vorabprüfungen überspringen**, wenn Sie nicht überprüfen möchten, ob der Plug-In-Host die Anforderungen für die Aktualisierung des Plug-Ins erfüllt.
    - iii. Klicken Sie auf **Upgrade**.
  - Wenn Sie mehrere Hosts aktualisieren möchten, wählen Sie alle Hosts aus, klicken Sie auf  und klicken Sie dann auf **Upgrade > OK**.

Alle zugehörigen Dienste werden während des Plug-In-Upgrades neu gestartet.



Alle Plug-Ins im Paket werden ausgewählt, aber nur die Plug-Ins, die mit der früheren Version von SnapCenter installiert wurden, werden aktualisiert, und die restlichen Plug-Ins werden nicht installiert. Sie müssen die Option **Plug-ins hinzufügen** verwenden, um ein neues Plug-in zu installieren.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird überprüft, ob der Plug-in-Host die Voraussetzungen für die Installation des Plug-ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen

angezeigt. Klicken Sie nach der Behebung des Problems auf **Upgrade**.



Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie entweder die web.config unter C:\Programme\ NetApp\ SnapCenter WebApp oder die PowerShell-Konfigurationsdateien unter C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter\ aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit verbleibenden Parametern zusammenhängt, müssen Sie das Problem beheben und die Anforderungen anschließend erneut validieren.



# Technische Aktualisierung

## Technische Aktualisierung des SnapCenter Server-Hosts

Wenn der SnapCenter Server-Host aktualisiert werden muss, können Sie dieselbe Version von SnapCenter Server auf dem neuen Host installieren und dann die APIs ausführen, um das SnapCenter vom alten Server zu sichern und auf dem neuen Server wiederherzustellen.

### Schritte

1. Stellen Sie den neuen Host bereit und führen Sie die folgenden Aufgaben aus:
  - a. Installieren Sie dieselbe Version des SnapCenter -Servers.
  - b. (Optional) Konfigurieren Sie CA-Zertifikate und aktivieren Sie bidirektionales SSL. Weitere Informationen finden Sie unter ["CA-Zertifikat konfigurieren"](#) Und ["Konfigurieren und Aktivieren von bidirektionalem SSL"](#) .
  - c. (Optional) Konfigurieren Sie die Multi-Faktor-Authentifizierung. Weitere Informationen finden Sie unter ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#) .
2. Melden Sie sich als SnapCenter -Administratorbenutzer an.
3. Erstellen Sie mithilfe der API eine Sicherung des SnapCenter -Servers auf dem alten Host:  
`/<snapcenter_version>/server/backup` oder das Cmdlet: *New-SmServerBackup*.



Unterbrechen Sie vor der Sicherung alle geplanten Jobs und stellen Sie sicher, dass keine Jobs ausgeführt werden.



Wenn Sie die Sicherung auf dem SnapCenter -Server wiederherstellen möchten, der auf einer neuen Domäne ausgeführt wird, sollten Sie vor der Erstellung einer Sicherung den neuen Domänenbenutzer im alten SnapCenter Host hinzufügen und ihm die SnapCenter Administratorrolle zuweisen.

4. Kopieren Sie das Backup vom alten Host auf den neuen Host.
5. Stellen Sie die Sicherung des SnapCenter -Servers auf dem neuen Host mithilfe der API wieder her:  
`/<snapcenter_version>/server/restore` oder das Cmdlet: *Restore-SmServerBackup*.

Durch die Wiederherstellung wird die neue SnapCenter -Server-URL standardmäßig auf allen Hosts aktualisiert. Wenn Sie das Update überspringen möchten, verwenden Sie das Attribut *-SkipSMSURLInHosts* und aktualisieren Sie die Server-URL separat, indem Sie entweder die folgende API verwenden: `/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.



Wenn der Plug-In-Host den Server-Hostnamen nicht auflösen kann, melden Sie sich bei jedem Plug-In-Host an und fügen Sie den Eintrag *etc/host* für die neue IP im Format `<Neue IP> SC_Server_Name` hinzu.



Die Server-*etc/Host*--Einträge werden nicht wiederhergestellt. Sie können es manuell vom alten Server wiederherstellen.

Wenn die Sicherung auf dem SnpCenter-Server wiederhergestellt wird, der auf einer neuen Domäne

ausgeführt wird, und Sie die alten Domänenbenutzer weiterhin verwenden möchten, sollten Sie die alte Domäne auf dem neuen SnapCenter -Server registrieren.



Wenn Sie die Datei web.config im alten SnapCenter -Host manuell aktualisiert haben, werden die Updates nicht auf den neuen Host kopiert. Sie sollten dieselben Änderungen manuell in der Datei web.config des neuen Hosts vornehmen.

6. Wenn Sie die Aktualisierung der SnapCenter -Server-URL übersprungen haben oder einer der Hosts während des Wiederherstellungsvorgangs ausgefallen war, aktualisieren Sie den neuen Servernamen in allen Hosts oder angegebenen Hosts, die vom SnapCenter verwaltet werden, mithilfe der API: `/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.
7. Aktivieren Sie die geplanten Jobs auf allen Hosts vom neuen SnapCenter -Server.

## Technische Aktualisierung eines Knotens im F5-Cluster

Sie können die technische Aktualisierung jedes Knotens im F5-Cluster durchführen, indem Sie den Knoten entfernen und den neuen Knoten hinzufügen. Wenn der Knoten, der aktualisiert werden muss, aktiv ist, machen Sie einen anderen Knoten des Clusters zum aktiven Knoten und entfernen Sie dann den Knoten.

Informationen zum Hinzufügen eines Knotens zum F5-Cluster finden Sie unter ["Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit mit F5"](#).



Wenn sich die URL des F5-Clusters ändert, kann die URL in allen Hosts mithilfe der API aktualisiert werden: `/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.

## Außerbetriebnahme des alten SnapCenter Server-Hosts

Sie können den alten SnapCenter Server-Host entfernen, nachdem Sie überprüft haben, dass der neue SnapCenter Server betriebsbereit ist und alle Plug-In-Hosts mit dem neuen SnapCenter Server-Host kommunizieren können.

## Rollback zum alten SnapCenter Server-Host

Bei Problemen können Sie den alten SnapCenter Server-Host wiederherstellen, indem Sie die SnapCenter Server-URL in allen Hosts mithilfe der API aktualisieren:

`/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.

## Notfallwiederherstellung

### Notfallwiederherstellung eines eigenständigen SnapCenter Hosts

Sie können eine Notfallwiederherstellung durchführen, indem Sie die Serversicherung auf dem neuen Host wiederherstellen.

#### Bevor Sie beginnen

Stellen Sie sicher, dass Sie über eine Sicherungskopie des alten SnapCenter -Servers verfügen.

#### Schritte

1. Stellen Sie den neuen Host bereit und führen Sie die folgenden Aufgaben aus:
  - a. Installieren Sie dieselbe Version des SnapCenter -Servers.

- b. Konfigurieren Sie CA-Zertifikate und aktivieren Sie bidirektionales SSL. Weitere Informationen finden Sie unter ["CA-Zertifikat konfigurieren"](#) Und ["Konfigurieren und Aktivieren von bidirektionalem SSL"](#) .
2. Kopieren Sie das alte SnapCenter Server-Backup auf den neuen Host.
3. Melden Sie sich als SnapCenter -Administratorbenutzer an.
4. Stellen Sie die Sicherung des SnapCenter -Servers auf dem neuen Host mithilfe der API wieder her:  
`/<snapcenter_version>/server/restore` oder das Cmdlet: *Restore-SmServerBackup*.

Durch die Wiederherstellung wird die neue SnapCenter -Server-URL standardmäßig auf allen Hosts aktualisiert. Wenn Sie das Update überspringen möchten, verwenden Sie das Attribut *-SkipSMSURLInHosts* und aktualisieren Sie die Server-URL separat, indem Sie entweder die API verwenden: `/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.



Wenn der Plug-In-Host den Server-Hostnamen nicht auflösen kann, melden Sie sich bei jedem Plug-In-Host an und fügen Sie den Eintrag *etc/host* für die neue IP im Format <Neue IP> SC\_Server\_Name hinzu.



Die Server-*etc/Host*--Einträge werden nicht wiederhergestellt. Sie können es manuell vom alten Server wiederherstellen.

5. Wenn Sie die Aktualisierung der URL übersprungen haben oder einer der Hosts während des Wiederherstellungsvorgangs ausgefallen war, aktualisieren Sie den neuen Servernamen in allen Hosts oder angegebenen Hosts, die vom SnapCenter verwaltet werden, mithilfe der API:  
`/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.

## Notfallwiederherstellung des SnapCenter F5-Clusters

Sie können eine Notfallwiederherstellung durchführen, indem Sie die Serversicherung auf dem neuen Host wiederherstellen und dann den eigenständigen Host in einen Cluster konvertieren.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie über eine Sicherungskopie des alten SnapCenter -Servers verfügen.

### Schritte

1. Stellen Sie den neuen Host bereit und führen Sie die folgenden Aufgaben aus:
  - a. Installieren Sie dieselbe Version des SnapCenter -Servers.
  - b. Konfigurieren Sie CA-Zertifikate und aktivieren Sie bidirektionales SSL. Weitere Informationen finden Sie unter ["CA-Zertifikat konfigurieren"](#) Und ["Konfigurieren und Aktivieren von bidirektionalem SSL"](#) .
2. Kopieren Sie das alte SnapCenter Server-Backup auf den neuen Host.
3. Melden Sie sich als SnapCenter -Administratorbenutzer an.
4. Stellen Sie die Sicherung des SnapCenter -Servers auf dem neuen Host mithilfe der API wieder her:  
`/<snapcenter_version>/server/restore` oder das Cmdlet: *Restore-SmServerBackup*.

Durch die Wiederherstellung wird die neue SnapCenter -Server-URL standardmäßig auf allen Hosts aktualisiert. Wenn Sie das Update überspringen möchten, verwenden Sie das Attribut *-SkipSMSURLInHosts* und aktualisieren Sie die Server-URL separat, indem Sie entweder die API verwenden: `/<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.



Wenn der Plug-In-Host den Server-Hostnamen nicht auflösen kann, melden Sie sich bei jedem Plug-In-Host an und fügen Sie den Eintrag *etc/host* für die neue IP im Format <Neue IP> SC\_Server\_Name hinzu.



Die Server-*etc/Host*--Einträge werden nicht wiederhergestellt. Sie können es manuell vom alten Server wiederherstellen.

5. Wenn Sie die Aktualisierung der URL übersprungen haben oder einer der Hosts während des Wiederherstellungsvorgangs ausgefallen war, aktualisieren Sie den neuen Servernamen in allen Hosts oder angegebenen Hosts, die vom SnapCenter verwaltet werden, mithilfe der API:  
/`<snapcenter_version>/server/configureurl` oder das Cmdlet: *Set-SmServerConfig*.
6. Konvertieren Sie den eigenständigen Host in einen F5-Cluster.

Informationen zur Konfiguration von F5 finden Sie unter ["Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit mit F5"](#).

### Ähnliche Informationen

Informationen zu den APIs erhalten Sie auf der Swagger-Seite. Siehe ["So greifen Sie über die Swagger-API-Webseite auf REST-APIs zu"](#).

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command\_name*. Alternativ können Sie auch die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

## Technische Aktualisierung der SnapCenter -Plug-in-Hosts

Wenn die SnapCenter -Plug-In-Hosts aktualisiert werden müssen, sollten Sie die Ressourcen vom alten Host auf den neuen Host verschieben. Wenn der neue Host zu SnapCenter hinzugefügt wird, erkennt er alle Ressourcen, wird aber als neue Ressourcen behandelt.

### Informationen zu diesem Vorgang

Sie sollten die API oder das Cmdlet ausführen, das den alten und den neuen Hostnamen als Eingabe verwendet, die Ressourcen nach Namen vergleicht und die Objekte der übereinstimmenden Ressourcen vom alten Host zum neuen Host neu verknüpft. Die passenden Ressourcen werden als geschützt markiert.

- Der Parameter *IsDryRun* ist standardmäßig auf True gesetzt und identifiziert die übereinstimmenden Ressourcen des alten und neuen Hosts.

Nachdem Sie die übereinstimmenden Ressourcen überprüft haben, sollten Sie den Parameter *IsDryRun* auf „False“ setzen, um die Objekte der übereinstimmenden Ressourcen vom alten Host mit dem neuen Host neu zu verknüpfen.

- Der Parameter *AutoMigrateManuallyAddedResources* ist standardmäßig auf „True“ gesetzt und kopiert die manuell hinzugefügten Ressourcen automatisch vom alten Host auf den neuen Host.

Der Parameter *AutoMigrateManuallyAddedResources* ist nur für Oracle- und SAP HANA-Ressourcen anwendbar.

- Der Parameter *SQLInstanceMapping* sollte verwendet werden, wenn der Instanzname zwischen dem alten und dem neuen Host unterschiedlich ist. Wenn es sich um eine Standardinstanz handelt, verwenden Sie

*default\_instance* als Instanznamen.

Die technische Aktualisierung wird für die folgenden SnapCenter -Plug-Ins unterstützt:

- SnapCenter -Plug-in für Microsoft SQL Server
  - Wenn die SQL-Datenbanken auf Instanzebene geschützt sind und im Rahmen der technischen Aktualisierung des Hosts nur Teile der Ressourcen auf einen neuen Host verschoben werden, wird der vorhandene Schutz auf Instanzebene in einen Ressourcengruppenschutz umgewandelt und Instanzen beider Hosts werden der Ressourcengruppe hinzugefügt.
  - Wenn ein SQL-Host (z. B. Host1) als Scheduler oder Verifizierungsserver für Ressourcen eines anderen Hosts (z. B. Host2) verwendet wird, werden der Zeitplan oder die Verifizierungsdetails während der Durchführung der technischen Aktualisierung auf Host1 nicht migriert und weiterhin auf Host1 ausgeführt. Wenn Sie Änderungen vornehmen müssen, sollten Sie diese manuell in den jeweiligen Hosts ändern.
  - Wenn Sie das Setup von SQL Failover Cluster Instances (FCI) verwenden, können Sie die technische Aktualisierung durchführen, indem Sie den neuen Knoten zum FCI-Cluster hinzufügen und den Plug-In-Host in SnapCenter aktualisieren.
  - Wenn Sie das SQL Availability Group (AG)-Setup verwenden, ist keine technische Aktualisierung erforderlich. Sie können den neuen Knoten zu AG hinzufügen und den Host in SnapCenter aktualisieren.
- SnapCenter -Plug-in für Windows
- SnapCenter -Plug-in für Oracle-Datenbank

Wenn Sie das Oracle Real Application Cluster (RAC)-Setup verwenden, können Sie die technische Aktualisierung durchführen, indem Sie den neuen Knoten zum RAC-Cluster hinzufügen und den Plug-In-Host in SnapCenter aktualisieren.

- SnapCenter Plug-in für SAP HANA-Datenbank

Die unterstützten Anwendungsfälle sind:

- Migrieren von Ressourcen von einem Host zu einem anderen Host.
- Migrieren von Ressourcen von mehreren Hosts auf einen oder weniger Hosts.
- Migrieren von Ressourcen von einem Host auf mehrere Hosts.

Die unterstützten Szenarien sind:

- Der neue Host hat einen anderen Namen als der alte Host
- Der vorhandene Host wurde umbenannt

### **Bevor Sie beginnen**

Da dieser Workflow die Daten im SnapCenter Repository ändert, wird empfohlen, das SnapCenter -Repository zu sichern. Im Falle von Datenproblemen kann das SnapCenter Repository mithilfe der Sicherung auf den alten Zustand zurückgesetzt werden.

Weitere Informationen finden Sie unter ["Sichern Sie das SnapCenter Repository"](#) .

### **Schritte**

1. Stellen Sie den neuen Host bereit und installieren Sie die Anwendung.
2. Setzen Sie die Zeitpläne des alten Hosts aus.

3. Verschieben Sie die erforderlichen Ressourcen vom alten Host auf den neuen Host.

a. Rufen Sie die erforderlichen Datenbanken im neuen Host aus demselben Speicher auf.

- Stellen Sie sicher, dass der Speicher demselben Laufwerk oder demselben Bereitstellungspfad wie der des alten Hosts zugeordnet ist. Wenn der Speicher nicht richtig zugeordnet ist, können auf dem alten Host erstellte Sicherungen nicht zur Wiederherstellung verwendet werden.



Standardmäßig weist Windows automatisch das nächste verfügbare Laufwerk zu.

- Wenn Storage DR aktiviert ist, sollte der entsprechende Speicher im neuen Host gemountet werden.

b. Überprüfen Sie die Kompatibilität, wenn sich die Anwendungsversion ändert.

c. Stellen Sie nur für den Oracle-Plug-in-Host sicher, dass die UIDs und GIDs von Oracle und seinen Gruppenbenutzern mit denen des alten Hosts übereinstimmen.

Weitere Informationen finden Sie unter:

- ["So migrieren Sie eine SQL-Datenbank vom alten Host auf einen neuen Host"](#)
- ["So migrieren Sie die Oracle-Datenbank vom alten Host auf den neuen Host"](#)
- ["So bringen Sie die SAP HANA-Datenbank auf einen neuen Host"](#)

4. Fügen Sie den neuen Host zu SnapCenter hinzu.

5. Überprüfen Sie, ob alle Ressourcen erkannt wurden.

6. Führen Sie die Host-Refresh-API aus: `/<snapcenter_version>/techrefresh/host` oder das Cmdlet: *Invoke-SmTechRefreshHost*.



Der Probelauf ist standardmäßig aktiviert und die passenden Ressourcen, die erneut verknüpft werden sollen, werden identifiziert. Sie können die Ressourcen überprüfen, indem Sie entweder die API „/jobs/{jobid}“ oder das Cmdlet *Get-SmJobSummaryReport* ausführen.

Wenn Sie die Ressourcen von mehreren Hosts migriert haben, sollten Sie die API oder das Cmdlet für alle Hosts ausführen. Wenn das Laufwerk oder der Mount-Pfad auf dem neuen Host nicht mit dem auf dem alten Host übereinstimmt, schlagen die folgenden Wiederherstellungsvorgänge fehl:

- Die SQL-In-Place-Wiederherstellung schlägt fehl. Die RTAL-Funktion kann jedoch genutzt werden.
- Die Wiederherstellung von Oracle- und SAP HANA-Datenbanken schlägt fehl.

Wenn Sie auf mehrere Hosts migrieren möchten, sollten Sie alle Schritte ab Schritt 1 für alle Hosts ausführen.



Sie können die API oder das Cmdlet mehrmals auf demselben Host ausführen. Die Verknüpfung wird nur dann erneut hergestellt, wenn eine neue Ressource identifiziert wird.

7. (Optional) Entfernen Sie den oder die alten Hosts aus SnapCenter.

### Ähnliche Informationen

Informationen zu den APIs erhalten Sie auf der Swagger-Seite. Siehe ["So greifen Sie über die Swagger-API-Webseite auf REST-APIs zu"](#).

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie

durch Ausführen von *Get-Help command\_name*. Alternativ können Sie auch die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Technische Aktualisierung des Speichersystems

Wenn der Speicher technisch aktualisiert wird, werden die Daten auf einen neuen Speicher migriert und die Anwendungshosts mit neuem Speicher gemountet. Der SnapCenter Sicherungsworkflow identifiziert den neuen Speicher und erstellt den Snapshot, wenn der neue Speicher in SnapCenter registriert ist.

Sie können die nach der Speicheraktualisierung erstellten neuen Sicherungen wiederherstellen, mounten und klonen. Diese Vorgänge schlagen jedoch fehl, wenn sie für die Sicherungen ausgeführt werden, die vor der Speicheraktualisierung erstellt wurden, da die Sicherungen die alten Speicherdetails enthalten. Sie sollten die Storage Tech Refresh-API oder das Cmdlet ausführen, um die alten Backups in SnapCenter mit den neuen Speicherdetails zu aktualisieren.

Die technische Aktualisierung wird für die folgenden SnapCenter -Plug-Ins unterstützt:

- SnapCenter -Plug-in für Microsoft SQL Server
- SnapCenter -Plug-in für Windows
- SnapCenter -Plug-in für Oracle-Datenbank
- SnapCenter Plug-in für SAP HANA-Datenbank
- SnapCenter -Plug-in für Microsoft Exchange Server

Die unterstützten Anwendungsfälle sind:

- Aktualisierung des primären Speichers

Die Aktualisierung der Speichertechnologie wird unterstützt, um den primären Speicher durch neuen Speicher zu ersetzen. Sie können den vorhandenen Sekundärspeicher nicht in einen Primärspeicher umwandeln.

- Aktualisierung des Sekundärspeichers

### Aktualisieren Sie die Backups des primären Speichers

Wenn der Speicher technisch aktualisiert wird, sollten Sie die API oder das Cmdlet zur technischen Aktualisierung des Speichers ausführen, um die alten Sicherungen in SnapCenter mit den neuen Speicherdetails zu aktualisieren.

#### Bevor Sie beginnen

Da dieser Workflow die Daten im SnapCenter Repository ändert, wird empfohlen, das SnapCenter -Repository zu sichern. Im Falle von Datenproblemen kann das SnapCenter Repository mithilfe der Sicherung auf den alten Zustand zurückgesetzt werden.

Weitere Informationen finden Sie unter ["Sichern Sie das SnapCenter Repository"](#) .

#### Schritte

1. Migrieren Sie die Daten vom alten Speicher zum neuen Speicher.

Informationen zur Migration finden Sie unter:



- "So migrieren Sie die Daten auf einen neuen Speicher"
- "Wie kann ich ein Volume kopieren und alle Snapshot-Kopien beibehalten?"

2. Versetzen Sie den Host in den Wartungsmodus.
3. Mounten Sie den neuen Speicher in den jeweiligen Hosts und rufen Sie die Datenbanken auf.

Der neue Speicher sollte auf die gleiche Weise wie zuvor mit dem Host verbunden werden. Wenn es beispielsweise als SAN verbunden war, muss es als SAN verbunden werden.

Der neue Speicher muss auf demselben Laufwerk oder Pfad wie der alte Speicher gemountet werden.

4. Stellen Sie sicher, dass alle Ressourcen betriebsbereit sind.
5. Fügen Sie den neuen Speicher in SnapCenter hinzu.

Stellen Sie sicher, dass Sie in allen Clustern in SnapCenter über einen eindeutigen SVM-Namen verfügen. Wenn Sie im neuen Speicher denselben SVM-Namen verwenden und alle Volumes des SVM migriert werden können, bevor die Speicheraktualisierung ausgeführt wird, wird empfohlen, das SVM im alten Cluster zu löschen und das alte Cluster in SnapCenter erneut zu ermitteln, wodurch das SVM aus dem Cache entfernt wird.

6. Versetzen Sie den Host in den Produktionsmodus.
7. Erstellen Sie in SnapCenter eine Sicherung der Ressourcen, deren Speicher migriert wird. Für SnapCenter ist eine neue Sicherung erforderlich, um den neuesten Speicherbedarf zu ermitteln. Außerdem wird sie zum Aktualisieren der Metadaten vorhandener alter Sicherungen verwendet.



Immer wenn eine neue LUN an den Host angeschlossen wird, erhält sie eine neue Seriennummer. Während der Erkennung des Windows-Dateisystems behandelt SnapCenter jede eindeutige Seriennummer als neue Ressource. Wenn während der Aktualisierung der Speichertechnologie die LUN aus dem neuen Speicher mit demselben Laufwerksbuchstaben oder Pfad an den Host angeschlossen wird, markiert die Erkennung des Windows-Dateisystems in SnapCenter die vorhandene Ressource als gelöscht, auch wenn sie mit demselben Laufwerksbuchstaben oder Pfad bereitgestellt wird, und zeigt die neue LUN als neue Ressource an. Da die Ressource als gelöscht markiert ist, wird sie für die Aktualisierung der Speichertechnologie in SnapCenter nicht berücksichtigt und alle Sicherungen der alten Ressource gehen verloren. Bei jeder Speicheraktualisierung sollte für Windows-Dateisystemressourcen die Ressourcenerkennung nicht vor der Ausführung der API oder des Cmdlets zur Speicheraktualisierung durchgeführt werden.

8. Führen Sie entweder die Speicheraktualisierungs-API aus:  
`/<snapcenter_version>/techrefresh/primarystorage` oder das Cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.



Wenn die Ressource mit einer replikationsfähigen Richtlinie konfiguriert ist, sollte die letzte Sicherung nach der Speicheraktualisierung Details zum sekundären Speicher enthalten.

- a. Wenn Sie das SQL Failover Cluster Instances (FCI)-Setup verwenden, werden die Sicherungen auf Clusterebene verwaltet. Sie sollten den Clusternamen als Eingabe für die Aktualisierung der Speichertechnologie angeben.
- b. Wenn Sie das SQL Availability Group (AG)-Setup verwenden, werden die Sicherungen auf Knotenebene verwaltet. Sie sollten den Knotennamen als Eingabe für die Aktualisierung der Speichertechnologie angeben.



- c. Wenn Sie das Oracle Real Application Clusters (RAC)-Setup verwenden, können Sie auf jedem Knoten eine Aktualisierung der Speichertechnologie durchführen.

Das Attribut *IsDryRun* ist standardmäßig auf True gesetzt. Es werden die Ressourcen identifiziert, für die der Speicher aktualisiert wird. Sie können die Ressource und die geänderten Speicherdetails anzeigen, indem Sie entweder die API „<snapcenter\_version>/jobs/{jobid}“ oder das Cmdlet „*Get-SmJobSummaryReport*“ ausführen.

9. Nachdem Sie die Speicherdetails überprüft haben, setzen Sie das Attribut *IsDryRun* auf „False“ und führen Sie die API zur Speicheraktualisierung aus:

/<snapcenter\_version>/techrefresh/primarystorage oder das Cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

Dadurch werden die Speicherdetails in den älteren Sicherungen aktualisiert.

Sie können die API oder das Cmdlet mehrmals auf demselben Host ausführen. Die Speicherdetails in den älteren Sicherungen werden nur aktualisiert, wenn der Speicher aktualisiert wird.



Die Klonhierarchie kann in ONTAP nicht migriert werden. Wenn der migrierte Speicher Klonmetadaten in SnapCenter enthält, wird die geklonte Ressource als unabhängige Ressource markiert. Klone von Klonmetadaten werden rekursiv entfernt.

10. (Optional) Wenn nicht alle Snapshots vom alten Primärspeicher in den neuen Primärspeicher verschoben werden, führen Sie die folgende API aus:

/<snapcenter\_version>/hosts/primarybackupsexistencecheck oder das Cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

Dadurch wird die Existenzprüfung des Snapshots auf dem neuen Primärspeicher durchgeführt und die entsprechenden Backups werden für keinen Vorgang in SnapCenter als verfügbar markiert.

## Aktualisieren Sie die Backups des sekundären Speichers

Wenn der Speicher technisch aktualisiert wird, sollten Sie die API oder das Cmdlet zur technischen Aktualisierung des Speichers ausführen, um die alten Sicherungen in SnapCenter mit den neuen Speicherdetails zu aktualisieren.

### Bevor Sie beginnen

Da dieser Workflow die Daten im SnapCenter Repository ändert, wird empfohlen, das SnapCenter -Repository zu sichern. Im Falle von Datenproblemen kann das SnapCenter Repository mithilfe der Sicherung auf den alten Zustand zurückgesetzt werden.

Weitere Informationen finden Sie unter ["Sichern Sie das SnapCenter Repository"](#) .

### Schritte

1. Migrieren Sie die Daten vom alten Speicher zum neuen Speicher.

Informationen zur Migration finden Sie unter:

- ["So migrieren Sie die Daten auf einen neuen Speicher"](#)
- ["Wie kann ich ein Volume kopieren und alle Snapshot-Kopien beibehalten?"](#)

2. Stellen Sie die SnapMirror -Beziehung zwischen dem primären Speicher und dem neuen sekundären Speicher her und stellen Sie sicher, dass der Beziehungsstatus in Ordnung ist.

3. Erstellen Sie in SnapCenter eine Sicherung der Ressourcen, deren Speicher migriert wird.

Für SnapCenter ist eine neue Sicherung erforderlich, um den neuesten Speicherbedarf zu ermitteln und sie wird zum Aktualisieren der Metadaten vorhandener alter Sicherungen verwendet.



Sie sollten warten, bis dieser Vorgang abgeschlossen ist. Wenn Sie vor Abschluss mit dem nächsten Schritt fortfahren, gehen alte sekundäre Snapshot-Metadaten vollständig verloren.

4. Nachdem Sie erfolgreich eine Sicherung aller Ressourcen auf einem Host erstellt haben, führen Sie entweder die API zur Aktualisierung des sekundären Speichers aus:

`/<snapcenter_version>/techrefresh/secondarystorage` oder das Cmdlet: *Invoke-SmTechRefreshSecondaryStorage*.

Dadurch werden die sekundären Speicherdetails der älteren Sicherungen auf dem angegebenen Host aktualisiert.

Wenn Sie dies auf Ressourcenebene ausführen möchten, klicken Sie für jede Ressource auf **Aktualisieren**, um die Metadaten des sekundären Speichers zu aktualisieren.

5. Nachdem Sie die älteren Sicherungen erfolgreich aktualisiert haben, können Sie die alte Beziehung zwischen dem sekundären und dem primären Speicher trennen.

# Deinstallieren Sie SnapCenter Server und Plug-Ins

## Deinstallieren Sie SnapCenter Plug-In-Pakete

### Voraussetzungen für das Entfernen eines Hosts

Sie können Hosts entfernen und einzelne Plug-Ins oder Plug-In-Pakete über die SnapCenter -GUI deinstallieren. Sie können einzelne Plug-Ins oder Plug-In-Pakete auf Remote-Hosts auch über die Befehlszeilenschnittstelle (CLI) auf Ihrem SnapCenter Server-Host oder über die Windows-Option **Programm deinstallieren** lokal auf einem beliebigen Host deinstallieren.

Bevor Sie einen Host vom SnapCenter Server entfernen, sollten Sie die Voraussetzungen erfüllen.

- Sie sollten sich als Administrator anmelden.
- Sie sollten sicherstellen, dass auf dem Host keine Erkennungsjobs ausgeführt werden.
- Ihnen sollte eine Rolle mit den erforderlichen Berechtigungen zugewiesen werden, um alle mit dem Host verknüpften Objekte zu entfernen. Andernfalls schlägt der Entfernungsvorgang fehl.
- Sie sollten den Fingerabdruck bestätigen, wenn der SSH-Schlüssel nach dem Hinzufügen des Hosts zu SnapCenter geändert wurde.
- Sie sollten den Fingerabdruck bestätigen, wenn der SnapCenter Host auf eine neuere Version von SnapCenter aktualisiert wird, auf dem Plug-In-Host jedoch noch eine frühere Version des Plug-Ins ausgeführt wird.

### Voraussetzungen zum Entfernen eines Hosts mithilfe der rollenbasierten Zugriffskontrolle

- Sie sollten sich mit einer RBAC-Rolle angemeldet haben, die über die Berechtigungen zum Lesen, Löschen von Hosts, Installieren, Deinstallieren von Plug-Ins und Löschen von Objekten verfügt.

Objekte können Klone, Backups, Ressourcengruppen, Speichersysteme usw. sein.

- Sie sollten den RBAC-Benutzer zur RBAC-Rolle hinzugefügt haben.
- Sie sollten den RBAC-Benutzer dem Host, dem Plug-In, den Anmeldeinformationen, den Ressourcengruppen und dem Speichersystem (für Klone) zuweisen, die Sie löschen möchten.
- Sie sollten sich bei SnapCenter als RBAC-Benutzer angemeldet haben.

### Voraussetzungen zum Entfernen eines Hosts mit Klonen, die aus dem Klon-Lebenszyklusvorgang erstellt wurden

- Sie sollten Klonjobs mithilfe der Klon-Lebenszyklusverwaltung für SQL-Datenbanken erstellt haben.
- Sie sollten eine RBAC-Rolle mit den Berechtigungen „Klon lesen und löschen“, „Ressourcen lesen und löschen“, „Ressourcengruppe lesen und löschen“, „Speicher lesen und löschen“, „Provision lesen und löschen“, „Mounten“, „Unmounten“, „Plugin installieren und deinstallieren“ sowie „Host lesen und löschen“ erstellt haben.
- Sie sollten dem RBAC-Benutzer die RBAC-Rolle zugewiesen haben.
- Sie sollten den RBAC-Benutzer dem Host, dem SnapCenter -Plug-in für Microsoft SQL Server, den

Anmeldeinformationen, der Klon-Lebenszyklus-Ressourcengruppe und dem Speichersystem zugewiesen haben.

- Sie sollten sich bei SnapCenter als RBAC-Benutzer angemeldet haben.

Informationen zum Deinstallieren des SnapCenter Plug-in for VMware vSphere finden Sie unter ["Entfernen Sie das SnapCenter Plug-in for VMware vSphere"](#) .

## Einen Host entfernen

Wenn der SnapCenter -Server einen Host entfernt, entfernt er zuerst die Sicherung, Klone, Klonjobs, Ressourcengruppen und Ressourcen, die für diesen Host auf der SnapCenter Ressourcenseite aufgeführt sind, und deinstalliert dann die Plug-In-Pakete auf dem Host.

### Informationen zu diesem Vorgang

- Wenn Sie einen Host löschen, werden auch die mit dem Host verknüpften Backups, Klone und Ressourcengruppen gelöscht.
- Wenn Sie die Ressourcengruppen entfernen, werden auch alle zugehörigen Zeitpläne entfernt.
- Wenn der Host über eine Ressourcengruppe verfügt, die mit einem anderen Host gemeinsam genutzt wird, und Sie den Host löschen, wird auch die Ressourcengruppe gelöscht.
- Sie sollten das Cmdlet *Remove-SmHost* verwenden, um die außer Betrieb genommenen oder nicht erreichbaren Plug-In-Hosts zu entfernen.

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"](#)

- Die zum Entfernen eines Hosts erforderliche Zeit hängt von der Anzahl der Sicherungen und den Aufbewahrungseinstellungen ab. Dies liegt daran, dass die Snapshots von jedem der Controller gelöscht und die Metadaten bereinigt werden.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite **Hosts** auf **Verwaltete Hosts**.
3. Wählen Sie den Host aus, den Sie entfernen möchten, und klicken Sie dann auf **Entfernen**.
4. Um bei Oracle RAC-Clustern die SnapCenter software von allen Hosts im Cluster zu entfernen, wählen Sie **Alle Hosts des Clusters einschließen**.

Sie können auch einen Knoten eines Clusters entfernen und auf diese Weise alle Knoten nacheinander entfernen.

5. Klicken Sie auf **OK**.



Wenn Sie Host-Plug-Ins auf einem Cluster deinstallieren und neu installieren, werden die Cluster-Ressourcen nicht automatisch erkannt. Wählen Sie den Cluster-Hostnamen aus und klicken Sie dann auf **Ressourcen aktualisieren**, um die Cluster-Ressourcen automatisch zu erkennen.

## Deinstallieren Sie Plug-Ins über die SnapCenter -GUI

Wenn Sie entscheiden, dass Sie ein einzelnes Plug-In oder ein Plug-In-Paket nicht mehr benötigen, können Sie es über die SnapCenter Schnittstelle deinstallieren.

### Bevor Sie beginnen

- Sie sollten die Ressourcengruppen für das Plug-In-Paket entfernt haben, das Sie deinstallieren.
- Sie sollten die mit den Ressourcengruppen verknüpften Richtlinien für das Plug-In-Paket, das Sie deinstallieren, getrennt haben.

### Informationen zu diesem Vorgang

Sie können einzelne Plug-ins deinstallieren. Beispielsweise müssen Sie möglicherweise das SnapCenter -Plug-in für Microsoft SQL Server deinstallieren, weil einem Host die Ressourcen ausgehen und Sie das Plug-in auf einen leistungsstärkeren Host verschieben möchten. Sie können auch ein ganzes Plug-In-Paket deinstallieren. Beispielsweise müssen Sie möglicherweise das SnapCenter Plug-ins-Paket für Linux deinstallieren, das das SnapCenter Plug-in für Oracle Database und das SnapCenter Plug-in für UNIX enthält.

- Das Entfernen eines Hosts umfasst die Deinstallation aller Plug-Ins.

Wenn Sie einen Host aus SnapCenter entfernen, deinstalliert SnapCenter alle Plug-In-Pakete auf dem Host, bevor der Host entfernt wird.

- Die SnapCenter -GUI entfernt Plug-Ins jeweils von einem Host.

Wenn Sie die SnapCenter -GUI verwenden, können Sie Plug-Ins jeweils nur auf einem Host deinstallieren. Sie können jedoch mehrere Deinstallationsvorgänge gleichzeitig ausführen.

Sie können ein Plug-In auch von mehreren Hosts deinstallieren, indem Sie das Cmdlet *Uninstall-SmHostPackage* und die erforderlichen Parameter verwenden. 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"](#).



Durch die Deinstallation des SnapCenter Plug-Ins-Pakets für Windows von einem Host, auf dem der SnapCenter Server installiert ist, wird die SnapCenter Server-Installation beschädigt. Deinstallieren Sie das SnapCenter Plug-ins-Paket für Windows nicht, es sei denn, Sie sind sicher, dass Sie den SnapCenter -Server nicht mehr benötigen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, von dem Sie das Plug-in oder Plug-in-Paket deinstallieren möchten.
4. Klicken Sie neben dem Plug-In, das Sie entfernen möchten, auf **Entfernen > Senden**.

### Nach Abschluss

Sie sollten 5 Minuten warten, bevor Sie das Plug-In auf diesem Host neu installieren. Dieser Zeitraum reicht aus, damit die SnapCenter GUI den Status des verwalteten Hosts aktualisieren kann. Die Installation schlägt fehl, wenn Sie das Plug-In sofort neu installieren.

Wenn Sie das SnapCenter Plug-ins-Paket für Linux deinstallieren, stehen deinstallationsspezifische

Protokolldateien unter `/custom_location/snapcenter/log` zur Verfügung.

## Deinstallieren Sie Windows-Plug-Ins mit dem PowerShell-Cmdlet

Sie können einzelne Plug-Ins oder Plug-In-Pakete von einem oder mehreren Hosts deinstallieren, indem Sie das Cmdlet *Uninstall-SmHostPackage* auf der Befehlszeilenschnittstelle des SnapCenter Server-Hosts verwenden.

Sie sollten sich auf jedem Host, auf dem Sie die Plug-Ins deinstallieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

### Schritte

1. Starten Sie PowerShell.
2. Geben Sie auf dem SnapCenter Server-Host den Befehl *Open-SMConnection -SMSbaseUrl https://SNAPCENTER\_SERVER\_NAME/DOMAIN\_NAME* ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Deinstallieren Sie die Windows-Plugins mit dem Cmdlet *Uninstall-SmHostPackage* und den erforderlichen Parametern.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command\_name*. Alternativ können Sie auch die ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#) .

## Plug-Ins lokal auf einem Host deinstallieren

Sie können SnapCenter -Plug-Ins lokal auf einem Host deinstallieren, wenn Sie den Host vom SnapCenter -Server aus nicht erreichen können.

### Informationen zu diesem Vorgang

Die bewährte Methode zum Deinstallieren einzelner Plug-Ins oder Plug-In-Pakete besteht darin, entweder die SnapCenter GUI oder das Cmdlet „Uninstall-SmHostPackage“ auf der Befehlszeilenschnittstelle des SnapCenter -Server-Hosts zu verwenden. Diese Verfahren helfen dem SnapCenter -Server, bei allen Änderungen auf dem neuesten Stand zu bleiben.

In seltenen Fällen kann es jedoch erforderlich sein, Plug-Ins lokal zu deinstallieren. Beispielsweise haben Sie möglicherweise einen Deinstallationsauftrag vom SnapCenter -Server ausgeführt, der jedoch fehlgeschlagen ist, oder Sie haben Ihren SnapCenter -Server deinstalliert und verwaiste Plug-Ins verbleiben auf einem Host.



Durch die lokale Deinstallation eines Plug-In-Pakets auf einem Host werden die mit dem Host verknüpften Daten, beispielsweise geplante Jobs und Sicherungsmetadaten, nicht gelöscht.



Versuchen Sie nicht, das SnapCenter Plug-ins-Paket für Windows lokal über die Systemsteuerung zu deinstallieren. Sie müssen die SnapCenter -GUI verwenden, um sicherzustellen, dass das SnapCenter -Plug-in für Microsoft Windows ordnungsgemäß deinstalliert wird.

### Schritte

1. Navigieren Sie auf dem Hostsystem zur Systemsteuerung und klicken Sie auf **Programm deinstallieren**.
2. Wählen Sie in der Programmliste das SnapCenter Plug-in oder Plug-in-Paket aus, das Sie deinstallieren möchten, und klicken Sie auf **Deinstallieren**.

Windows deinstalliert alle Plug-Ins im ausgewählten Paket.

## Deinstallieren Sie das Plug-In-Paket für Linux oder AIX mithilfe der CLI

Sie können das SnapCenter Plug-ins Package für Linux oder das SnapCenter Plug-ins Package für AIX über die Befehlszeilenschnittstelle deinstallieren.

### Bevor Sie beginnen

- Stellen Sie sicher, dass Sie die geplanten Jobs gelöscht haben
- Stellen Sie sicher, dass alle laufenden Jobs abgeschlossen sind.

### Schritt

Führen Sie zum Deinstallieren `/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall` aus.

## Deinstallieren Sie den SnapCenter -Server auf dem Windows-Host

Wenn Sie den SnapCenter Server nicht mehr zum Verwalten von Datenschutzaufträgen verwenden möchten, können Sie den SnapCenter Server über die Systemsteuerung „Programme und Funktionen“ auf dem SnapCenter Server-Host deinstallieren. Durch die Deinstallation des SnapCenter -Servers werden alle seine Komponenten entfernt.

### Bevor Sie beginnen

- Stellen Sie sicher, dass auf dem Laufwerk, auf dem der SnapCenter -Server installiert ist, mindestens 2 GB freier Speicherplatz vorhanden sind.
- Stellen Sie sicher, dass die Domäne, in der der SnapCenter -Server installiert ist, nicht entfernt wird.

Wenn Sie die Domäne entfernen, in der der SnapCenter -Server installiert war, und dann versuchen, ihn zu deinstallieren, schlägt der Vorgang fehl.

- Sie sollten die Repository-Datenbank gesichert haben, da die Repository-Datenbank bereinigt und deinstalliert wird.

### Schritte

1. Navigieren Sie auf dem SnapCenter Server-Host zur Systemsteuerung.
2. Stellen Sie sicher, dass Sie sich in der **Kategorie**-Ansicht befinden.
3. Klicken Sie unter „Programme“ auf „Programm deinstallieren“.

Das Fenster „Programme und Funktionen“ wird geöffnet.

4. Wählen Sie NetApp SnapCenter Server aus und klicken Sie dann auf **Deinstallieren**.

Wenn Sie ab SnapCenter 4.2 den SnapCenter -Server deinstallieren, werden alle seine Komponenten einschließlich der MySQL-Server-Repository-Datenbank deinstalliert.

- Zum Entfernen des NLB-Knotens aus einem NLB-Cluster müssen Sie den SnapCenter Server-Host neu starten. Wenn Sie den Host nicht neu starten, kann es beim Versuch, den SnapCenter -Server neu zu installieren, zu einem Fehler kommen.

- Sie sollten .NET Framework manuell deinstallieren, da es bei der Deinstallation nicht entfernt wird.

## Deinstallieren Sie den SnapCenter -Server auf dem Linux-Host

Wenn Sie den SnapCenter Server nicht mehr zum Verwalten von Datenschutzaufträgen verwenden möchten, können Sie den SnapCenter Server deinstallieren. Durch die Deinstallation des SnapCenter -Servers werden alle seine Komponenten entfernt.

### Schritte

1. Führen Sie eine der Aktionen aus, um SnapCenter Server zu deinstallieren.

| Wenn Sie auftreten möchten ...   | Machen Sie Folgendes...                                                                                                                                                                                                    |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nicht interaktive Deinstallation | <pre>\$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1</pre> <p>Beispiel: <code>sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</code></p>                      |
| Interaktive Deinstallation       | <pre>\$ sudo &lt;USER_INSTALL_DIR&gt;/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</pre> <p>Geben Sie in der Bestätigungseingabe einen beliebigen Wert ungleich 0 ein, um die Deinstallation zu bestätigen.</p> |



# Automatisieren Sie mit REST-APIs

## SnapCenter -Automatisierung mithilfe von REST-APIs

Sie können REST-APIs verwenden, um verschiedene SnapCenter -Verwaltungsvorgänge durchzuführen. REST-APIs werden über die Swagger-Webseite bereitgestellt. Sie können auf die Swagger-Webseite unter

`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` zugreifen, um die REST-API-Dokumentation anzuzeigen und manuell einen API-Aufruf zu tätigen.

Die Plug-Ins, die REST-APIs unterstützen, sind:

- Plug-in für Microsoft SQL Server
- Plug-in für SAP HANA-Datenbank
- Plug-in für Oracle-Datenbank

Informationen zum SnapCenter Plug-in for VMware vSphere REST APIs finden Sie unter ["SnapCenter Plug-in for VMware vSphere REST-APIs"](#)

## So greifen Sie nativ auf die SnapCenter REST-API zu

Sie können mit jeder Programmiersprache, die einen REST-Client unterstützt, direkt auf die SnapCenter REST-API zugreifen. Zu den beliebten Sprachen gehören Python, PowerShell und Java.

## REST-Webdienstgrundlagen

Representational State Transfer (REST) ist ein Stil zur Erstellung verteilter Webanwendungen. Bei der Entwicklung einer Webservice-API etabliert es eine Reihe von Technologien und Best Practices für die Bereitstellung serverbasierter Ressourcen und die Verwaltung ihrer Zustände. Es verwendet gängige Protokolle und Standards, um eine flexible Grundlage für die Verwaltung von SnapCenter bereitzustellen.

### Ressourcen und staatliche Vertretung

Ressourcen sind die grundlegenden Komponenten eines webbasierten Systems. Zu den ersten Entwurfsaufgaben beim Erstellen einer REST-Webdienstanwendung gehören:

#### Identifizierung system- oder serverbasierter Ressourcen

Jedes System verwendet und verwaltet Ressourcen. Eine Ressource kann eine Datei, eine Geschäftstransaktion, ein Prozess oder eine Verwaltungseinheit sein. Eine der ersten Aufgaben beim Entwurf einer Anwendung auf Basis von REST-Webdiensten ist die Identifizierung der Ressourcen.

#### Definition von Ressourcenzuständen und zugehörigen Zustandsoperationen

Ressourcen befinden sich immer in einem von einer begrenzten Anzahl von Zuständen. Die Zustände sowie die zugehörigen Operationen, die zur Beeinflussung der Zustandsänderungen verwendet werden, sollten klar

definiert sein.

## URI-Endpunkte

Jede REST-Ressource muss mithilfe eines klar definierten Adressierungsschemas definiert und bereitgestellt werden. Die Endpunkte, an denen die Ressourcen lokalisiert und identifiziert werden, verwenden einen Uniform Resource Identifier (URI).

Der URI bietet einen allgemeinen Rahmen für die Erstellung eines eindeutigen Namens für jede Ressource im Netzwerk. Der Uniform Resource Locator (URL) ist ein URI-Typ, der in Webdiensten zur Identifizierung und zum Zugriff auf Ressourcen verwendet wird. Ressourcen werden typischerweise in einer hierarchischen Struktur ähnlich einem Dateiverzeichnis bereitgestellt.

## HTTP-Nachrichten

HTTP (Hypertext Transfer Protocol) ist das Protokoll, das vom Webdienst-Client und -Server zum Austausch von Anforderungs- und Antwortnachrichten zu Ressourcen verwendet wird.

Beim Entwurf einer Webdienstanwendung werden HTTP-Methoden den Ressourcen und den entsprechenden Aktionen zur Statusverwaltung zugeordnet. HTTP ist zustandslos. Um eine Reihe zusammengehöriger Anfragen und Antworten als Teil einer Transaktion zu verknüpfen, müssen daher zusätzliche Informationen in die HTTP-Header aufgenommen werden, die mit den Anfrage- und Antwortdatenflüssen übertragen werden.

## JSON-Formatierung

Informationen können auf verschiedene Weise strukturiert und zwischen einem Webdienst-Client und einem Server übertragen werden, die beliebteste Option ist jedoch JavaScript Object Notation (JSON).

JSON ist ein Industriestandard für die Darstellung einfacher Datenstrukturen in Klartext und wird zur Übertragung von Statusinformationen verwendet, die die Ressourcen beschreiben. Die SnapCenter REST-API verwendet JSON, um die im Text jeder HTTP-Anfrage und -Antwort enthaltenen Daten zu formatieren.

# Grundlegende Betriebsmerkmale

REST bietet zwar einen gemeinsamen Satz an Technologien und Best Practices, die Details der einzelnen APIs können jedoch je nach Designentscheidung variieren.

## Anforderungs- und Antwort-API-Transaktion

Jeder REST-API-Aufruf wird als HTTP-Anfrage an das SnapCenter -Serversystem ausgeführt, das eine zugehörige Antwort an den Client generiert. Dieses Anforderungs- und Antwortpaar wird als API-Transaktion betrachtet.

Bevor Sie die API verwenden, sollten Sie mit den zur Steuerung einer Anfrage verfügbaren Eingabevariablen und dem Inhalt der Antwortausgabe vertraut sein.

## Unterstützung für CRUD-Operationen

Der Zugriff auf jede der über die SnapCenter REST-API verfügbaren Ressourcen erfolgt basierend auf dem CRUD-Modell:

- Erstellen

- Lesen
- Aktualisieren
- Löschen

Für einige Ressourcen wird nur eine Teilmenge der Vorgänge unterstützt.

## Objektkennungen

Jede Ressourceninstanz oder jedes Objekt erhält bei der Erstellung eine eindeutige Kennung. In den meisten Fällen ist die Kennung eine 128-Bit-UUID. Diese Kennungen sind innerhalb eines bestimmten SnapCenter Servers global eindeutig.

Nach dem Ausführen eines API-Aufrufs, der eine neue Objektinstanz erstellt, wird dem Aufrufer im Location-Header der HTTP-Antwort eine URL mit der zugehörigen ID zurückgegeben. Sie können die Kennung extrahieren und sie bei nachfolgenden Aufrufen verwenden, wenn Sie auf die Ressourceninstanz verweisen.



Inhalt und interne Struktur der Objektkennungen können sich jederzeit ändern. Sie sollten die Kennungen bei den entsprechenden API-Aufrufen nur nach Bedarf verwenden, wenn Sie auf die zugehörigen Objekte verweisen.

## Objektinstanzen und Sammlungen

Abhängig vom Ressourcenpfad und der HTTP-Methode kann ein API-Aufruf für eine bestimmte Objektinstanz oder eine Sammlung von Objekten gelten.

## Synchrone und asynchrone Vorgänge

SnapCenter führt eine von einem Client empfangene HTTP-Anfrage entweder synchron oder asynchron aus.

### Synchrone Verarbeitung

SnapCenter führt die Anfrage sofort aus und antwortet bei Erfolg mit einem HTTP-Statuscode von 200 oder 201.

Jede Anfrage mit der Methode GET wird immer synchron ausgeführt. Darüber hinaus sind Anfragen, die POST verwenden, so konzipiert, dass sie synchron ausgeführt werden, wenn ihre Fertigstellung in weniger als zwei Sekunden erwartet wird.

### Asynchrone Verarbeitung

Wenn eine asynchrone Anforderung gültig ist, erstellt SnapCenter eine Hintergrundaufgabe zur Verarbeitung der Anforderung und ein Jobobjekt zur Verankerung der Aufgabe. Der HTTP-Statuscode 202 wird zusammen mit dem Jobobjekt an den Anrufer zurückgegeben. Sie sollten den Status des Auftrags abrufen, um Erfolg oder Misserfolg festzustellen.

Anfragen, die die Methoden POST und DELETE verwenden, werden asynchron ausgeführt, wenn ihre Ausführung voraussichtlich mehr als zwei Sekunden dauert.

## Sicherheit

Die mit der REST-API bereitgestellte Sicherheit basiert hauptsächlich auf den vorhandenen Sicherheitsfunktionen, die mit SnapCenter verfügbar sind. Die API verwendet die folgende Sicherheit:

## Transportschichtssicherheit

Der gesamte über das Netzwerk zwischen dem SnapCenter -Server und dem Client gesendete Datenverkehr wird normalerweise basierend auf den SnapCenter -Konfigurationseinstellungen mit TLS verschlüsselt.

## HTTP-Authentifizierung

Auf HTTP-Ebene wird für die API-Transaktionen eine grundlegende Authentifizierung verwendet. Jeder Anfrage wird ein HTTP-Header mit dem Benutzernamen und dem Passwort in einer Base64-Zeichenfolge hinzugefügt.

# Eingabevariablen, die eine API-Anfrage steuern

Sie können die Verarbeitung eines API-Aufrufs über in der HTTP-Anforderung festgelegte Parameter und Variablen steuern.

## HTTP-Methoden

Die von der SnapCenter REST-API unterstützten HTTP-Methoden sind in der folgenden Tabelle aufgeführt.



Nicht alle HTTP-Methoden sind an jedem REST-Endpunkt verfügbar.

| HTTP-Methode | Beschreibung                                                                     |
|--------------|----------------------------------------------------------------------------------|
| ERHALTEN     | Ruft Objekteigenschaften einer Ressourceninstanz oder -sammlung ab.              |
| POST         | Erstellt eine neue Ressourceninstanz basierend auf der bereitgestellten Eingabe. |
| LÖSCHEN      | Löscht eine vorhandene Ressourceninstanz.                                        |
| SETZEN       | Ändert eine vorhandene Ressourceninstanz.                                        |

## Anforderungsheader

Sie sollten mehrere Header in die HTTP-Anfrage aufnehmen.

### Inhaltstyp

Wenn der Anforderungstext JSON enthält, sollte dieser Header auf *application/json* gesetzt werden.

### Akzeptieren

Dieser Header sollte auf *application/json* gesetzt werden.

### Genehmigung

Die Basisauthentifizierung sollte mit dem als Base64-Zeichenfolge codierten Benutzernamen und Kennwort eingerichtet werden.

## Anforderungstext

Der Inhalt des Anforderungstexts variiert je nach Aufruf. Der HTTP-Anforderungstext besteht aus einem der folgenden Elemente:

- JSON-Objekt mit Eingabevariablen
- Leer

## Objekte filtern

Wenn Sie einen API-Aufruf mit GET ausführen, können Sie die zurückgegebenen Objekte basierend auf einem beliebigen Attribut einschränken oder filtern. Sie können beispielsweise einen genauen Wert angeben, der übereinstimmen soll:

`<field>=<query value>`

Zusätzlich zu einer exakten Übereinstimmung stehen weitere Operatoren zur Verfügung, um eine Menge von Objekten über einen Wertebereich zurückzugeben. Die SnapCenter REST API unterstützt die in der folgenden Tabelle aufgeführten Filteroperatoren.

| Operator      | Beschreibung           |
|---------------|------------------------|
| =             | Gleich                 |
| <             | Weniger als            |
| >             | Größer als             |
| ≤             | Kleiner oder gleich    |
| ≥             | Größer als oder gleich |
| AKTUALISIEREN | Oder                   |
| !             | Ungleich               |
| *             | Geringer Platzhalter   |

Sie können auch eine Sammlung von Objekten zurückgeben, basierend darauf, ob ein bestimmtes Feld festgelegt ist oder nicht, indem Sie das Schlüsselwort **null** oder seine Negation **!null** als Teil der Abfrage verwenden.



Alle nicht festgelegten Felder werden grundsätzlich von übereinstimmenden Abfragen ausgeschlossen.

## Anfordern bestimmter Objektfelder

Standardmäßig gibt ein API-Aufruf mit GET nur die Attribute zurück, die das Objekt bzw. die Objekte eindeutig identifizieren. Dieser Mindestsatz an Feldern dient als Schlüssel für jedes Objekt und variiert je nach Objekttyp. Weitere Objekteigenschaften können Sie über die `fields` Abfrageparameter auf folgende Weise:

### Gemeinsame oder Standardfelder

Geben Sie **fields=\*** an, um die am häufigsten verwendeten Objektfelder abzurufen. Diese Felder werden normalerweise im lokalen Serverspeicher verwaltet oder erfordern nur eine geringe Verarbeitung für den Zugriff. Dies sind dieselben Eigenschaften, die für ein Objekt zurückgegeben werden, nachdem GET mit einem

URL-Pfadsschlüssel (UUID) verwendet wurde.

## Alle Felder

Geben Sie **fields=\*\*** an, um alle Objektfelder abzurufen, einschließlich derjenigen, für deren Zugriff zusätzliche Serververarbeitung erforderlich ist.

## Benutzerdefinierte Feldauswahl

Verwenden Sie **fields=<Feldname>**, um das gewünschte Feld genau anzugeben. Wenn Sie mehrere Felder anfordern, müssen die Werte durch Kommas und ohne Leerzeichen getrennt werden.



Als Best Practice sollten Sie immer die gewünschten Felder angeben. Sie sollten den Satz gemeinsamer Felder oder alle Felder nur bei Bedarf abrufen. Welche Felder als gemeinsam klassifiziert und mit *fields=\** zurückgegeben werden, wird von NetApp anhand einer internen Leistungsanalyse ermittelt. Die Klassifizierung eines Feldes kann sich in zukünftigen Versionen ändern.

## Sortieren von Objekten im Ausgabesatz

Die Datensätze einer Ressourcensammlung werden in der vom Objekt definierten Standardreihenfolge zurückgegeben. Sie können die Reihenfolge ändern, indem Sie `order_by` Abfrageparameter mit dem Feldnamen und der Sortierrichtung wie folgt:

```
order_by=<field name> asc|desc
```

Sie können beispielsweise das Typfeld in absteigender Reihenfolge und anschließend die ID in aufsteigender Reihenfolge sortieren:

```
order_by=type desc, id asc
```

- Wenn Sie ein Sortierfeld angeben, aber keine Richtung angeben, werden die Werte in aufsteigender Reihenfolge sortiert.
- Wenn Sie mehrere Parameter angeben, müssen Sie die Felder durch ein Komma trennen.

## Seitennummerierung beim Abrufen von Objekten in einer Sammlung

Wenn Sie einen API-Aufruf mit GET ausgeben, um auf eine Sammlung von Objekten desselben Typs zuzugreifen, versucht SnapCenter, basierend auf zwei Einschränkungen so viele Objekte wie möglich zurückzugeben. Sie können jede dieser Einschränkungen mithilfe zusätzlicher Abfrageparameter in der Anfrage steuern. Die erste für eine bestimmte GET-Anforderung erreichte Einschränkung beendet die Anforderung und begrenzt daher die Anzahl der zurückgegebenen Datensätze.



Wenn eine Anfrage endet, bevor alle Objekte durchlaufen wurden, enthält die Antwort den Link, der zum Abrufen des nächsten Datensatzstapels erforderlich ist.

## Begrenzung der Anzahl der Objekte

Standardmäßig gibt SnapCenter maximal 10.000 Objekte für eine GET-Anfrage zurück. Sie können dieses Limit mit dem Abfrageparameter *max\_records* ändern. Beispiel:

```
max_records=20
```

Die Anzahl der tatsächlich zurückgegebenen Objekte kann unter dem geltenden Maximum liegen, abhängig von der jeweiligen Zeitbeschränkung und der Gesamtzahl der Objekte im System.

### Begrenzung der zum Abrufen der Objekte benötigten Zeit

Standardmäßig gibt SnapCenter so viele Objekte wie möglich innerhalb der für die GET-Anfrage zulässigen Zeit zurück. Das Standard-Timeout beträgt 15 Sekunden. Sie können dieses Limit mit dem Abfrageparameter *return\_timeout* ändern. Beispiel:

```
return_timeout=5
```

Die Anzahl der tatsächlich zurückgegebenen Objekte kann geringer sein als das geltende Maximum, basierend auf der entsprechenden Einschränkung der Objektanzahl sowie der Gesamtzahl der Objekte im System.

### Eingrenzen des Ergebnissatzes

Bei Bedarf können Sie diese beiden Parameter mit zusätzlichen Abfrageparametern kombinieren, um den Ergebnissatz einzugrenzen. Beispielsweise gibt Folgendes bis zu 10 EMS-Ereignisse zurück, die nach der angegebenen Zeit generiert wurden:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Sie können mehrere Anfragen stellen, um durch die Objekte zu blättern. Jeder nachfolgende API-Aufruf sollte einen neuen Zeitwert basierend auf dem letzten Ereignis im letzten Ergebnissatz verwenden.

### Größeneigenschaften

Die bei einigen API-Aufrufen sowie bestimmten Abfrageparametern verwendeten Eingabewerte sind numerisch. Anstatt eine Ganzzahl in Bytes anzugeben, können Sie optional ein Suffix verwenden, wie in der folgenden Tabelle gezeigt.

| Suffix | Beschreibung                                |
|--------|---------------------------------------------|
| KB     | KB Kilobyte (1024 Byte) oder Kibibyte       |
| MB     | MB Megabyte (KB x 1024 Bytes) oder Mebibyte |
| GB     | GB Gigabyte (MB x 1024 Bytes) oder Gibibyte |
| TB     | TB Terabyte (GB x 1024 Byte) oder Tebibyte  |
| PB     | PB Petabyte (TB x 1024 Bytes) oder Pebibyte |

## Interpretation einer API-Antwort

Jede API-Anfrage generiert eine Antwort an den Client. Sie sollten die Antwort prüfen, um festzustellen, ob sie erfolgreich war, und bei Bedarf weitere Daten abrufen.

### HTTP-Statuscode

Die von der SnapCenter REST-API verwendeten HTTP-Statuscodes werden unten beschrieben.

| Code | Beschreibung                                                                                                                                                                |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 200  | OK: Zeigt den Erfolg von Aufrufen an, die kein neues Objekt erstellen.                                                                                                      |
| 201  | Erstellt. Ein Objekt wurde erfolgreich erstellt. Der Standortheader in der Antwort enthält die eindeutige Kennung für das Objekt.                                           |
| 202  | Akzeptiert. Ein Hintergrundjob wurde gestartet, um die Anfrage auszuführen, ist aber noch nicht abgeschlossen.                                                              |
| 400  | Ungültige Anfrage. Die Anfrageeingabe wird nicht erkannt oder ist ungeeignet.                                                                                               |
| 401  | Die Authentifizierung des nicht autorisierten Benutzers ist fehlgeschlagen.                                                                                                 |
| 403  | Der Zugriff wurde aufgrund eines Autorisierungsfehlers (RBAC) verweigert.                                                                                                   |
| 404  | Nicht gefunden. Die in der Anfrage genannte Ressource existiert nicht.                                                                                                      |
| 405  | Methode nicht zulässig. Die HTTP-Methode in der Anforderung wird für die Ressource nicht unterstützt.                                                                       |
| 409  | Konflikt: Ein Versuch, ein Objekt zu erstellen, ist fehlgeschlagen, weil zuerst ein anderes Objekt erstellt werden muss oder das angeforderte Objekt bereits vorhanden ist. |
| 500  | Interner Fehler. Auf dem Server ist ein allgemeiner interner Fehler aufgetreten.                                                                                            |

## Antwortheader

Die vom SnapCenter generierte HTTP-Antwort enthält mehrere Header.

### Standort

Wenn ein Objekt erstellt wird, enthält der Standortheader die vollständige URL zum neuen Objekt, einschließlich der dem Objekt zugewiesenen eindeutigen Kennung.

### Inhaltstyp

Dies wird normalerweise `application/json`.

## Antworttext

Der Inhalt des Antworttexts einer API-Anforderung unterscheidet sich je nach Objekt, Verarbeitungstyp und Erfolg oder Misserfolg der Anforderung. Die Antwort wird immer in JSON gerendert.

### Einzelnes Objekt

Basierend auf der Anfrage kann ein einzelnes Objekt mit einer Reihe von Feldern zurückgegeben werden.



Beispielsweise können Sie GET verwenden, um ausgewählte Eigenschaften eines Clusters mithilfe der eindeutigen Kennung abzurufen.

## Mehrere Objekte

Es können mehrere Objekte aus einer Ressourcensammlung zurückgegeben werden. In allen Fällen wird ein einheitliches Format verwendet, mit `num_records` Gibt die Anzahl der Datensätze und Datensätze an, die ein Array der Objektinstanzen enthalten. Sie können beispielsweise die in einem bestimmten Cluster definierten Knoten abrufen.

## Job-Objekt

Wenn ein API-Aufruf asynchron verarbeitet wird, wird ein Job-Objekt zurückgegeben, das die Hintergrundaufgabe verankert. Beispielsweise wird die PATCH-Anforderung zum Aktualisieren der Clusterkonfiguration asynchron verarbeitet und gibt ein Job-Objekt zurück.

## Fehlerobjekt

Wenn ein Fehler auftritt, wird immer ein Error-Objekt zurückgegeben. Beispielsweise erhalten Sie eine Fehlermeldung, wenn Sie versuchen, ein Feld zu ändern, das für einen Cluster nicht definiert ist.

## Leer

In bestimmten Fällen werden keine Daten zurückgegeben und der Antworttext enthält ein leeres JSON-Objekt.

## Fehler

Wenn ein Fehler auftritt, wird im Antworttext ein Fehlerobjekt zurückgegeben.

## Format

Ein Fehlerobjekt hat das folgende Format:

```
"error": {  
  "message": "<string>",  
  "code": <integer>[,  
  "target": "<string>"]  
}
```

Mithilfe des Codewerts können Sie den allgemeinen Fehlertyp oder die Kategorie bestimmen und anhand der Meldung den spezifischen Fehler ermitteln. Sofern verfügbar, enthält das Zielfeld die spezifische Benutzereingabe, die mit dem Fehler verknüpft ist.

## Häufige Fehlercodes

Die häufigsten Fehlercodes werden in der folgenden Tabelle beschrieben. Bestimmte API-Aufrufe können zusätzliche Fehlercodes enthalten.

| Code | Beschreibung                                            |
|------|---------------------------------------------------------|
| 409  | Ein Objekt mit derselben Kennung ist bereits vorhanden. |

| Code | Beschreibung                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------------|
| 400  | Der Wert für ein Feld hat einen ungültigen Wert oder fehlt, oder es wurde ein zusätzliches Feld bereitgestellt. |
| 400  | Der Vorgang wird nicht unterstützt.                                                                             |
| 405  | Ein Objekt mit der angegebenen Kennung kann nicht gefunden werden.                                              |
| 403  | Die Berechtigung zur Ausführung der Anfrage wird verweigert.                                                    |
| 409  | Die Ressource wird verwendet.                                                                                   |

## Für SnapCenter Server und Plug-Ins unterstützte REST-APIs

Die über die SnapCenter REST-API verfügbaren Ressourcen sind in Kategorien organisiert, wie auf der Dokumentationsseite der SnapCenter -API angezeigt. Nachfolgend finden Sie eine kurze Beschreibung der einzelnen Ressourcen mit den Basisressourcenpfaden sowie gegebenenfalls zusätzliche Hinweise zur Verwendung.

### Authentifizierung

Sie können diese API verwenden, um sich beim SnapCenter -Server anzumelden. Diese API gibt ein Benutzerautorisierungstoken zurück, das zur Authentifizierung nachfolgender Anfragen verwendet wird.

### Domänen

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle Domänen in SnapCenter abrufen
- Details einer bestimmten Domäne abrufen
- Registrieren oder Aufheben der Registrierung einer Domain
- Ändern einer Domäne

### Jobs

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle Jobs in SnapCenter abrufen
- Status eines Jobs abrufen
- einen Auftrag abbuchen oder stoppen

### Einstellungen

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Anmeldeinformationen registrieren, ändern oder entfernen
- zeigt die im SnapCenter Server registrierten Anmeldeinformationen an
- Benachrichtigungseinstellungen konfigurieren
- Ruft Informationen über den SMTP-Server ab, der aktuell für den Versand von E-Mail-Benachrichtigungen konfiguriert ist, und zeigt den Namen des SMTP-Servers, den Namen der Empfänger und den Namen des Absenders an.
- zeigt die Multi-Faktor-Authentifizierung (MFA)-Konfiguration der SnapCenter Server-Anmeldung an
- Aktivieren oder Deaktivieren und Konfigurieren von MFA für die SnapCenter Server-Anmeldung
- Erstellen Sie die zum Einrichten von MFA erforderliche Konfigurationsdatei

## Gastgeber

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle SnapCenter Hosts abfragen
- Entfernen Sie einen oder mehrere Hosts aus SnapCenter
- Abrufen eines Hosts nach Namen
- Abrufen aller Ressourcen auf einem Host
- Abrufen einer Ressource mithilfe der Ressourcen-ID
- Abrufen der Plug-in-Konfigurationsdetails
- Konfigurieren Sie den Plug-In-Host
- alle Ressourcen des Plug-ins für Microsoft SQL Server-Host abrufen
- alle Ressourcen des Plug-ins für den Oracle-Datenbankhost abrufen
- alle Ressourcen des Plug-ins für den benutzerdefinierten Anwendungshost abrufen
- alle Ressourcen des Plug-ins für den SAP HANA-Host abrufen
- die installierten Plug-Ins abrufen
- Installieren Sie Plug-Ins auf einem vorhandenen Host
- Upgrade des Host-Pakets
- Plug-Ins von einem vorhandenen Host entfernen
- Plug-In auf einem Host hinzufügen
- Host hinzufügen oder ändern
- Holen Sie sich die Signatur des Linux-Hosts
- Registrieren Sie die Signatur des Linux-Hosts
- den Host in den Wartungs- oder Produktionsmodus versetzen
- Starten oder starten Sie die Plug-In-Dienste auf dem Host
- Umbenennen eines Hosts

## Ressourcen

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle Ressourcen abrufen
- Abrufen einer Ressource mithilfe der Ressourcen-ID
- alle Ressourcen des Plug-ins für Microsoft SQL Server-Host abrufen
- alle Ressourcen des Plug-ins für den Oracle-Datenbankhost abrufen
- alle Ressourcen des Plug-ins für den benutzerdefinierten Anwendungshost abrufen
- alle Ressourcen des Plug-ins für den SAP HANA-Host abrufen
- Abrufen einer Microsoft SQL Server-Ressource mithilfe eines Schlüssels
- Abrufen einer benutzerdefinierten Ressource mithilfe eines Schlüssels
- Ändern Sie eine Ressource des Plug-Ins für einen benutzerdefinierten Anwendungshost
- Entfernen Sie eine Ressource des Plug-Ins für den benutzerdefinierten Anwendungshost mithilfe eines Schlüssels
- Abrufen einer SAP HANA-Ressource mithilfe eines Schlüssels
- Ändern Sie eine Ressource des Plug-Ins für den SAP HANA-Host
- Entfernen Sie eine Ressource des Plug-Ins für den SAP HANA-Host mithilfe eines Schlüssels
- Abrufen einer Oracle-Ressource mithilfe eines Schlüssels
- Erstellen Sie eine Oracle-Anwendungsvolume-Ressource
- Ändern einer Oracle-Anwendungsvolume-Ressource
- Entfernen einer Oracle-Anwendungsvolume-Ressource mithilfe eines Schlüssels
- Rufen Sie die sekundären Details der Oracle-Ressource ab
- Sichern Sie die Microsoft SQL Server-Ressource mit dem Plug-In für Microsoft SQL Server
- Sichern Sie die Oracle-Ressource mit dem Plug-In für die Oracle-Datenbank
- Sichern Sie die benutzerdefinierte Ressource mithilfe des Plug-Ins für benutzerdefinierte Anwendungen
- Konfigurieren der SAP HANA-Datenbank
- Konfigurieren der Oracle-Datenbank
- Wiederherstellen einer SQL-Datenbanksicherung
- Wiederherstellen einer Oracle-Datenbanksicherung
- Wiederherstellen einer benutzerdefinierten Anwendungssicherung
- Erstellen einer SAP HANA-Ressource
- Schützen Sie eine benutzerdefinierte Ressource mithilfe eines Plug-Ins für benutzerdefinierte Anwendungen
- Schützen Sie eine Microsoft SQL Server-Ressource mit dem Plug-In für Microsoft SQL Server
- Ändern einer geschützten Microsoft SQL Server-Ressource
- Entfernen Sie den Schutz für die Microsoft SQL Server-Ressource
- Schützen Sie eine Oracle-Ressource mit dem Plug-In für die Oracle-Datenbank
- Ändern einer geschützten Oracle-Ressource
- Entfernen Sie den Schutz von der Oracle-Ressource
- Klonen Sie eine Ressource aus der Sicherung mithilfe des Plug-Ins für eine benutzerdefinierte Anwendung
- Klonen Sie ein Oracle-Anwendungsvolume aus der Sicherung mithilfe des Plug-Ins für die Oracle-

## Datenbank

- Klonen Sie eine Microsoft SQL Server-Ressource aus der Sicherung mithilfe des Plug-Ins für Microsoft SQL Server
- Erstellen Sie einen Klon-Lebenszyklus einer Microsoft SQL Server-Ressource
- Ändern des Klon-Lebenszyklus einer Microsoft SQL Server-Ressource
- Löschen des Klon-Lebenszyklus einer Microsoft SQL Server-Ressource
- Verschieben Sie eine vorhandene Microsoft SQL Server-Datenbank von einer lokalen Festplatte auf eine NetApp LUN
- Erstellen Sie eine Klonpezifikationsdatei für eine Oracle-Datenbank
- Initiieren Sie einen On-Demand-Klonaktualisierungsjob einer Oracle-Ressource
- Erstellen Sie mithilfe der Klonpezifikationsdatei eine Oracle-Ressource aus der Sicherung
- stellt die Datenbank auf dem sekundären Replikat wieder her und fügt die Datenbank wieder der Verfügbarkeitsgruppe hinzu
- Erstellen Sie eine Oracle-Anwendungsvolume-Ressource

## Backups

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Abrufen von Sicherungsdetails nach Sicherungsname, Typ, Plug-in, Ressource oder Datum
- alle Backups abrufen
- Abrufen von Sicherungsdetails
- Backups umbenennen oder löschen
- Mounten Sie ein Oracle-Backup
- Unmounten einer Oracle-Sicherung
- Katalogisieren Sie ein Oracle-Backup
- Dekatalogisieren Sie ein Oracle-Backup
- Holen Sie sich alle Backups, die für die Durchführung einer zeitpunktbezogenen Wiederherstellung bereitgestellt werden müssen

## Klone

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Erstellen, Anzeigen, Ändern und Löschen der Oracle-Datenbank-Klonpezifikationsdatei
- Oracle-Datenbank-Klonhierarchie anzeigen
- Klondetails abrufen
- alle Klone abrufen
- Klone löschen
- Abrufen von Klondetails nach ID
- Initiieren Sie einen On-Demand-Klonaktualisierungsjob einer Oracle-Ressource
- Klonen Sie eine Oracle-Ressource aus der Sicherung mithilfe der Klonpezifikationsdatei

## Klonaufteilung

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Schätzen Sie den Klon-Split-Vorgang der geklonten Ressource
- Abrufen des Status einer Klon-Split-Operation
- Starten oder Stoppen einer Klon-Teilungsoperation

## Ressourcengruppen

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Details aller Ressourcengruppen abrufen
- Rufen Sie die Ressourcengruppe nach Namen ab
- Erstellen Sie eine Ressourcengruppe für das Plug-In für eine benutzerdefinierte Anwendung
- Erstellen Sie eine Ressourcengruppe für das Plug-In für Microsoft SQL Server
- Erstellen Sie eine Ressourcengruppe für das Plug-In für die Oracle-Datenbank
- Ändern Sie eine Ressourcengruppe für das Plug-In für eine benutzerdefinierte Anwendung
- Ändern einer Ressourcengruppe für das Plug-In für Microsoft SQL Server
- Ändern Sie eine Ressourcengruppe für das Plug-In für die Oracle-Datenbank
- Erstellen, Ändern oder Löschen des Klon-Lebenszyklus einer Ressourcengruppe für das Plug-In für Microsoft SQL Server
- Sichern einer Ressourcengruppe
- Versetzen Sie die Ressourcengruppe in den Wartungs- oder Produktionsmodus
- Entfernen einer Ressourcengruppe

## Richtlinien

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Richtliniendetails abrufen
- Abrufen von Richtliniendetails nach Namen
- Löschen einer Richtlinie
- Erstellen Sie eine Kopie einer vorhandenen Richtlinie
- Erstellen oder Ändern einer Richtlinie für Plug-Ins für benutzerdefinierte Anwendungen
- Erstellen oder Ändern einer Richtlinie für das Plug-In für Microsoft SQL Server
- Erstellen oder Ändern der Richtlinie für Plug-In für Oracle-Datenbank
- Erstellen oder Ändern einer Richtlinie für das Plug-In für die SAP HANA-Datenbank

## Storage

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle Freigaben abrufen

- Abrufen einer Freigabe nach Namen
- Erstellen oder Löschen einer Freigabe
- Speicherdetails abrufen
- Abrufen von Speicherdetails nach Namen
- Erstellen, Ändern oder Löschen eines Speichers
- Ermitteln von Ressourcen auf einem Speichercluster
- Abrufen von Ressourcen auf einem Speichercluster

## Aktie

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- die Details einer Freigabe abrufen
- Details zu allen Aktien abrufen
- Erstellen oder Löschen einer Freigabe auf dem Speicher
- Abrufen einer Freigabe nach Namen

## Plugins

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle Plug-Ins für einen Host auflisten
- Abrufen einer Microsoft SQL Server-Ressource mithilfe eines Schlüssels
- Ändern einer benutzerdefinierten Ressource mithilfe eines Schlüssels
- Entfernen einer benutzerdefinierten Ressource mithilfe eines Schlüssels
- Abrufen einer SAP HANA-Ressource mithilfe eines Schlüssels
- Ändern einer SAP HANA-Ressource mithilfe eines Schlüssels
- Entfernen einer SAP HANA-Ressource mithilfe eines Schlüssels
- Abrufen einer Oracle-Ressource mithilfe eines Schlüssels
- Ändern einer Oracle-Anwendungsvolume-Ressource mithilfe eines Schlüssels
- Entfernen einer Oracle-Anwendungsvolume-Ressource mithilfe eines Schlüssels
- Sichern Sie die Microsoft SQL Server-Ressource mit dem Plug-in für Microsoft SQL Server und einem Schlüssel
- Sichern Sie die Oracle-Ressource mit dem Plug-In für die Oracle-Datenbank und einem Schlüssel
- Sichern Sie die benutzerdefinierte Anwendungsressource mithilfe des Plug-Ins für benutzerdefinierte Anwendungen und eines Schlüssels
- Konfigurieren Sie die SAP HANA-Datenbank mithilfe eines Schlüssels
- Konfigurieren Sie die Oracle-Datenbank mithilfe eines Schlüssels
- Wiederherstellen einer benutzerdefinierten Anwendungssicherung mithilfe eines Schlüssels
- Erstellen einer SAP HANA-Ressource
- Erstellen Sie eine Oracle-Anwendungsvolume-Ressource

- Schützen Sie eine benutzerdefinierte Ressource mithilfe eines Plug-Ins für benutzerdefinierte Anwendungen
- Schützen Sie eine Microsoft SQL Server-Ressource mit dem Plug-In für Microsoft SQL Server
- Ändern einer geschützten Microsoft SQL Server-Ressource
- Entfernen Sie den Schutz für die Microsoft SQL Server-Ressource
- Schützen Sie eine Oracle-Ressource mit dem Plug-In für die Oracle-Datenbank
- Ändern einer geschützten Oracle-Ressource
- Entfernen Sie den Schutz von der Oracle-Ressource
- Klonen Sie eine Ressource aus der Sicherung mithilfe des Plug-Ins für eine benutzerdefinierte Anwendung
- Klonen Sie ein Oracle-Anwendungsvolume aus der Sicherung mithilfe des Plug-Ins für die Oracle-Datenbank
- Klonen Sie eine Microsoft SQL Server-Ressource aus der Sicherung mithilfe des Plug-Ins für Microsoft SQL Server
- Erstellen Sie einen Klon-Lebenszyklus einer Microsoft SQL Server-Ressource
- Ändern des Klon-Lebenszyklus einer Microsoft SQL Server-Ressource
- Löschen des Klon-Lebenszyklus einer Microsoft SQL Server-Ressource
- Erstellen Sie eine Klonpezifikationsdatei für eine Oracle-Datenbank
- Initiieren Sie einen On-Demand-Klon-Lebenszyklus einer Oracle-Ressource
- Klonen Sie eine Oracle-Ressource aus der Sicherung mithilfe der Klonpezifikationsdatei

## Berichte

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Abrufen von Berichten über Sicherungs-, Wiederherstellungs- und Klonvorgänge für die jeweiligen Plug-Ins
- Zeitpläne hinzufügen, ausführen, löschen oder ändern
- Daten für die geplanten Berichte abrufen

## Warnungen

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- alle Warnungen abrufen
- Abrufen von Warnungen nach IDs
- mehrere Warnungen löschen oder eine Warnung nach ID löschen

## Rbac

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Details zu Benutzern, Gruppen und Rollen abrufen
- Benutzer hinzufügen oder löschen
- Benutzer einer Rolle zuweisen



- Benutzer von Rolle aufheben
- Rollen erstellen, ändern oder löschen
- Gruppe einer Rolle zuweisen
- Aufheben der Zuordnung einer Gruppe zu einer Rolle
- Gruppen hinzufügen oder löschen
- Erstellen Sie eine Kopie einer vorhandenen Rolle
- Zuweisen oder Aufheben der Zuweisung von Ressourcen zu Benutzern oder Gruppen

## Konfiguration

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Anzeigen der Konfigurationseinstellungen
- Ändern Sie die Konfigurationseinstellungen

## Zertifikateinstellungen

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- den Zertifikatsstatus für den SnapCenter -Server oder Plug-in-Host anzeigen
- Ändern Sie die Zertifikateinstellungen für den SnapCenter -Server oder den Plug-In-Host

## Archiv

Sie können APIs verwenden, um verschiedene Vorgänge auszuführen.

- Abrufen der Repository-Sicherungen
- die Konfigurationsinformationen zum Repository anzeigen
- Schützen und Wiederherstellen des SnapCenter Repository
- Schutz des SnapCenter Repository aufheben
- Repository neu erstellen und Failover durchführen

## Version

Sie können diese API verwenden, um die SnapCenter -Version anzuzeigen.

## So greifen Sie über die Swagger-API-Webseite auf REST-APIs zu

REST-APIs werden über die Swagger-Webseite bereitgestellt. Sie können auf die Swagger-Webseite zugreifen, um die REST-APIs des SnapCenter Servers anzuzeigen und manuell einen API-Aufruf zu tätigen. Sie können REST-APIs verwenden, um Ihren SnapCenter Server zu verwalten oder Datenschutzvorgänge durchzuführen.

Sie sollten die Verwaltungs-IP-Adresse oder den Domännennamen des SnapCenter -Servers kennen, auf dem Sie die REST-APIs ausführen möchten.

Sie benötigen keine besonderen Berechtigungen, um den REST-API-Client auszuführen. Jeder Benutzer kann auf die Swagger-Webseite zugreifen. Die jeweiligen Berechtigungen für die Objekte, auf die über die REST-API zugegriffen wird, basieren auf dem Benutzer, der das Token zur Anmeldung bei der REST-API generiert.

## Schritte

1. Geben Sie in einem Browser die URL zum Zugriff auf die Swagger-Webseite im Format `https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` ein.



Stellen Sie sicher, dass die REST-API-URL nicht die folgenden Zeichen enthält: +, ., %, und &.

2. Wenn die Swagger-API-Dokumentation nicht automatisch angezeigt wird, geben Sie im Feld **Swagger Explore** Folgendes ein:  
`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/ SnapCenter.yaml`

3. Klicken Sie auf **Erkunden**.

Es wird eine Liste mit API-Ressourcentypen oder -Kategorien angezeigt.

4. Klicken Sie auf einen API-Ressourcentyp, um die APIs in diesem Ressourcentyp anzuzeigen.

Wenn beim Ausführen von SnapCenter REST-APIs unerwartetes Verhalten auftritt, können Sie die Protokolldateien verwenden, um die Ursache zu ermitteln und das Problem zu beheben. Sie können die Protokolldateien von der SnapCenter -Benutzeroberfläche herunterladen, indem Sie auf **Überwachen > Protokolle > Herunterladen** klicken.

## Erste Schritte mit der REST-API

Mit der SnapCenter REST-API können Sie schnell loslegen. Der Zugriff auf die API bietet eine gewisse Perspektive, bevor Sie beginnen, sie mit den komplexeren Workflow-Prozessen in einem Live-Setup zu verwenden.

## Hallo Welt

Sie können einen einfachen Befehl auf Ihrem System ausführen, um mit der Verwendung der SnapCenter REST-API zu beginnen und ihre Verfügbarkeit zu bestätigen.

### Bevor Sie beginnen

- Stellen Sie sicher, dass das Curl-Dienstprogramm auf Ihrem System verfügbar ist.
- IP-Adresse oder Hostname des SnapCenter -Servers
- Benutzername und Kennwort für ein Konto mit Zugriffsberechtigung auf die SnapCenter REST-API.



Wenn Ihre Anmeldeinformationen Sonderzeichen enthalten, müssen Sie sie so formatieren, dass sie für Curl basierend auf der von Ihnen verwendeten Shell akzeptabel sind. Sie können beispielsweise vor jedem Sonderzeichen einen Backslash einfügen oder den gesamten `username:password` Zeichenfolge in einfachen Anführungszeichen.

### Schritt

Führen Sie in der Befehlszeilenschnittstelle Folgendes aus, um die Plug-In-Informationen abzurufen:

```
curl -X GET -u username:password -k
```

```
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Beispiel:

```
curl -X GET -u admin:password -k
```

```
"https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

# Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

## Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

["Hinweis zu SnapCenter 6.1"](#)

## Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.