SnapCenter-Softwaredokumentation

SnapCenter Software 6.0

NetApp
August 04, 2025

Inhalt

SnapCenter-Softwaredokumentation . . . 1
Versionshinweise . . . 2
Versionshinweise . . . 2
Unterstützte Upgrade-Pfade für SnapCenter . . . 2
Konzepte . . . 3
Übersicht über SnapCenter . . . 3
Architektur von SnapCenter . . . 6
Komponenten von SnapCenter . . . 6
SnapCenter Server . . . 7
SnapCenter Plug-ins . . . 8
SnapCenter Repository . . . 11
Sicherheitsfunktionen . . . 11
ÜBERSICHT ÜBER DAS CA-Zertifikat . . . 12
Bidirektionale SSL-Kommunikation . . . 13
Übersicht über die zertifikatbasierte Authentifizierung . . . 13
Multi-Faktor-Authentifizierung (MFA) . . . 13
Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter . . . 13
RBAC-Typen . . . 13
RBAC-Berechtigungen und -Rollen . . . 15
Vordefinierte SnapCenter-Rollen und -Berechtigungen . . . 16
SnapCenter Disaster Recovery . . . 20
Ressourcen, Ressourcengruppen und Richtlinien . . . 21
Vorschriften und Postskripte . . . 22
Unterstützte Skripttypen . . . 22
Skriptpfad . . . 23
Angeben von Skripten . . . 23
Skript-Timeouts . . . 23
Skriptausgabe . . . 23
SnapCenter-Automatisierung mit REST-APIs . . . 24
Installation von SnapCenter Server . . . 25
Installations-Workflow . . . 25
Bereiten Sie sich auf die Installation des SnapCenter-Servers vor . . . 25
Anforderungen an Domäne und Arbeitsgruppe . . . 25
Platz- und Größenanforderungen . . . 26
SAN-Host-Anforderungen . . . 28
Unterstützte Storage-Systeme und Applikationen . . . 28
Unterstützte Browser . . . 29
Verbindungs- und Portanforderungen . . . 29
SnapCenter-Lizenzen . . . 33
Registrieren Sie sich, um auf die SnapCenter Software zuzugreifen . . . 36
Authentifizierungsmethoden für Ihre Anmeldedaten . . . 37
Storage-Verbindungen und Anmeldedaten . . . 38
Multi-Faktor-Authentifizierung (MFA) . . . 39

Installieren Sie den SnapCenter-Server auf dem Windows-Host . . . 49
Registrieren Sie das Produkt, um den Support zu aktivieren . . . 50
Installieren Sie den SnapCenter-Server auf dem Linux-Host . . . 51
Registrieren Sie das Produkt, um den Support zu aktivieren . . . 55
Melden Sie sich über die RBAC-Autorisierung bei SnapCenter an . . . 55
Melden Sie sich mit Multi-Faktor-Authentifizierung (MFA) bei SnapCenter an. . . . 57
Ändern Sie das Zeitlimit für die SnapCenter-StandardGUI-Sitzung . . . 58
Sichern Sie den SnapCenter Webserver durch Deaktivieren von SSL 3.0 . . . 58
Konfigurieren Sie das CA-Zertifikat für den Windows-Host . . . 59
ZertifikatCSR-Datei erstellen . . . 59
Importieren von CA-Zertifikaten . . . 59
Abrufen des Daumenabdrucks für das CA-Zertifikat . . . 60
Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-in-Diensten . . . 60
Konfigurieren Sie ein CA-Zertifikat mit SnapCenter Site . . . 61
Aktivieren Sie CA-Zertifikate für SnapCenter . . . 62
Konfigurieren Sie das CA-Zertifikat für den Linux-Host . . . 63
Konfigurieren Sie das nginx-Zertifikat . . . 63
Konfigurieren Sie das Audit-Protokoll-Zertifikat . . . 63
Konfigurieren Sie das Zertifikat für SnapCenter-Services . . . 63
Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host . . . 64
Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host . . . 64
Aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host . . . 67
Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host . . . 68
Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host . . . 68
Aktivieren Sie die SSL-Kommunikation auf Linux-Host . . . 69
Konfigurieren Sie die zertifikatbasierte Authentifizierung . . . 70
Exportieren Sie Zertifikate der Zertifizierungsstelle (CA) vom SnapCenter-Server . . . 70
Zertifikat der Zertifizierungsstelle (CA) auf die Windows-Plug-in-Hosts importieren . . . 71
Importieren Sie das CA-Zertifikat in die UNIX-Host-Plug-ins, und konfigurieren Sie Root- oder Zwischenzertifikate in den SPL-Trust-Store . . . 72
Aktivieren Sie die zertifikatbasierte Authentifizierung . . . 73
Exportieren von SnapCenter-Zertifikaten . . . 74
Konfiguration von Active Directory, LDAP und LDAPS . . . 75
Registrieren Sie nicht vertrauenswürdige Active Directory-Domänen . . . 75
Konfigurieren Sie das CA-Client-Zertifikat für LDAPS . . . 76
Konfiguration Der Hochverfügbarkeit . . . 77
Konfigurieren Sie SnapCenter-Server für Hochverfügbarkeit . . . 77
Hochverfügbarkeit für das SnapCenter MySQL Repository . . . 81
Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) . . . 82
Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu . . . 82
Erstellen Sie eine Rolle . . . 85
Fügen Sie mithilfe von Sicherheits-Login-Befehlen eine ONTAP RBAC-Rolle hinzu . . . 85
Erstellen Sie SVM-Rollen mit minimalen Berechtigungen . . . 87
Erstellen Sie ONTAP-Cluster-Rollen mit minimalen Berechtigungen . . . 92
Konfigurieren Sie IIS-Anwendungspools, um die Leseberechtigungen von Active Directory zu

aktivieren . . . 98
Konfigurieren Sie die Einstellungen für das Prüfprotokoll . . . 99
Storage-Systeme hinzufügen . . . 100
Controller-basierte SnapCenter Standard-Lizenzen hinzufügen . . . 104
Schritt 1: Überprüfen Sie, ob die SnapManager Suite-Lizenz installiert ist . . . 104
Schritt 2: Identifizieren Sie die auf dem Controller installierten Lizenzen . . . 105
Schritt 3: Rufen Sie die Seriennummer des Controllers ab . . . 106
Schritt 4: Rufen Sie die Seriennummer der Controller-basierten Lizenz ab . . . 107
Schritt 5: Controller-basierte Lizenz hinzufügen . . . 108
Schritt 6: Entfernen Sie die Testlizenz . . . 109
Bereitstellung Ihres Storage-Systems . . . 109
Bereitstellen von Storage auf Windows Hosts . . . 109
Bereitstellung von Storage in VMware Umgebungen . . . 125
Konfigurieren Sie gesicherte MySQL-Verbindungen mit SnapCenter-Server . . . 128
Konfigurieren Sie gesicherte MySQL-Verbindungen für eigenständige SnapCenter-Server-Konfigurationen . . . 128
Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen . . . 130
Während der Installation auf Ihrem Windows-Host aktivierte Funktionen . . . 134
Funktionen, die während der Installation auf dem Linux-Host aktiviert wurden . . . 137
Microsoft SQL Server Datenbanken schützen . . . 138
SnapCenter Plug-in für Microsoft SQL Server . . . 138
SnapCenter Plug-in für Microsoft SQL Server – Übersicht . . . 138
Welche Möglichkeiten bietet das SnapCenter Plug-in für Microsoft SQL Server . . . 138
SnapCenter Plug-in für Microsoft SQL Server Funktionen . . . 139
Unterstützung für asymmetrische LUN-Zuordnung in Windows Clustern . . . 140
Vom SnapCenter-Plug-in für Microsoft SQL Server unterstützte Speichertypen . . . 141
Empfehlungen für das Storage-Layout für das SnapCenter Plug-in für Microsoft SQL Server . . . 144
Minimale ONTAP-Berechtigungen für SQL Plug-in erforderlich . . . 146
Storage-Systeme für SnapMirror und SnapVault Replizierung für Plug-in für SQL Server vorbereiten . . . 148
Backup-Strategie für SQL Server-Ressourcen . . . 149
Wiederherstellungsstrategie für SQL Server . . . 154
Definieren Sie eine Klonstrategie für SQL Server . . . 157
Bereiten Sie die Installation des SnapCenter-Plug-ins für Microsoft SQL Server vor . . . 158
Installations-Workflow für das SnapCenter Plug-in für Microsoft SQL Server . . . 158
Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter-Plug-ins für Microsoft SQL Server . . . 158
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows . . . 159
Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-ins-Paket für Windows ein . . . 160
Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource . . . 162
Konfigurieren Sie gMSA unter Windows Server 2016 oder höher . . . 165
Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server . . . 166
Konfigurieren Sie das CA-Zertifikat . . . 173
Konfiguration der Disaster Recovery . . . 176
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 178
Bereitstellen eines CA-Zertifikats . . . 179

Konfigurieren Sie die CRL-Datei . . . 179
Bereiten Sie sich auf die Datensicherung vor . . . 179
Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für Microsoft SQL Server . . . 179
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SQL Server verwendet werden 180
Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe . . . 181
Backup-Workflow . . . 181
Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind . . . 182
Migrieren von Ressourcen auf ein NetApp Storage-System . . . 184
Erstellen von Backup-Richtlinien für SQL Server-Datenbanken . . . 186
Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server . . . 194
Anforderungen für das Backup von SQL Ressourcen . . . 197
Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets . . . 197
Backup von SQL-Ressourcen . . . 198
Sichern Sie SQL Server-Ressourcengruppen . . . 204
Überwachen Sie die Backup-Vorgänge für SQL-Ressourcen auf der Seite SnapCenter-Jobs . . . 205
Abbrechen des SnapCenter-Plug-ins für Microsoft SQL Server-Backup-Vorgänge . . . 206
Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an . . . 207
Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets . . . 209
Stellen Sie SQL Server-Ressourcen wieder her . . . 210
Wiederherstellung des Workflows . . . 210
Anforderungen für das Wiederherstellen einer Datenbank . . . 210
Stellen Sie Backups von SQL Server Datenbanken wieder her . . . 212
Wiederherstellung einer SQL Server-Datenbank aus dem sekundären Storage . . . 219
Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her . . . 220
Datenbanken der Verfügbarkeitsgruppe erneut erstellen . . . 222
Überwachung von Restore-Vorgängen bei SQL-Ressourcen . . . 223
Wiederherstellungsvorgänge für SQL-Ressourcen abbrechen . . . 224
Klonen von SQL Server Datenbankressourcen . . . 225
Klon-Workflow . . . 225
Klonen aus einem Backup der SQL Server Datenbank . . . 226
Führen Sie Den Klon-Lebenszyklus Durch . . . 234
Überwachen Sie die Klonvorgänge von SQL Datenbanken . . . 237
Klonvorgänge für SQL-Ressourcen abbrechen . . . 238
Teilen Sie einen Klon auf . . . 238
Schutz von SAP HANA Datenbanken . . . 240
SnapCenter Plug-in für SAP HANA Datenbanken . . . 240
SnapCenter-Plug-in für SAP HANA-Datenbank – Überblick . . . 240
Was Sie mit dem SnapCenter Plug-in für SAP HANA Database tun können . . . 240
SnapCenter Plug-in für SAP HANA Database Funktionen . . . 240
Storage-Typen, die vom SnapCenter Plug-in für SAP HANA Database unterstützt werden . . . 241
Minimale ONTAP-Berechtigungen für SAP HANA-Plug-in erforderlich . . . 242
Vorbereiten der Storage-Systeme für SnapMirror und SnapVault Replizierung für SAP HANA Datenbanken . . . 245
Backup-Strategie für SAP HANA Datenbanken . . . 245
Restore- und Recovery-Strategie für SAP HANA Datenbanken . . . 249

Bereiten Sie sich auf die Installation des SnapCenter-Plug-ins für die SAP HANA-Datenbank vor 251
Installationsworkflow des SnapCenter Plug-ins für SAP HANA Database 251
Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter Plug-ins für SAP HANA Database 252
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows 255
Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux 256
Anmeldedaten für das SnapCenter-Plug-in für SAP HANA-Datenbank einrichten 257
Konfigurieren Sie gMSA unter Windows Server 2016 oder höher 260
Das SnapCenter-Plug-in für SAP HANA Datenbanken installieren 261
Konfigurieren Sie das CA-Zertifikat 267
Installieren Sie das SnapCenter Plug-in für VMware vSphere 275
Bereitstellen eines CA-Zertifikats 276
Konfigurieren Sie die CRL-Datei 276
Bereiten Sie sich auf die Datensicherung vor 276
Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für SAP HANA-Datenbanken 276
Verwendung von Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SAP HANA Datenbanken 277
SAP HANA-Ressourcen sichern 277
SAP HANA-Ressourcen sichern 277
Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank 278
Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor 279
Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu 282
Backup-Richtlinien für SAP HANA Datenbanken 284
Erstellen von Ressourcengruppen und Anhängen von Richtlinien 291
Erstellen einer Storage-Systemverbindung und einer Zertifizierung mit PowerShell cmdlets für SAP HANA Datenbank 295
SAP HANA Datenbanken sichern 297
Sichern von Ressourcengruppen 304
Monitoring von Backup-Vorgängen bei SAP HANA Datenbanken 304
Abbrechen der Backup-Vorgänge für SAP HANA 306
Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an 306
Wiederherstellung von SAP HANA Datenbanken 308
Wiederherstellung des Workflows 308
Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups 309
Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her 313
Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her 318
Überwachen von Restore-Vorgängen bei SAP HANA Datenbanken 320
Backups von SAP HANA Ressourcen klonen 321
Klon-Workflow 321
Klonen eines Backups einer SAP HANA Datenbank 322
Überwachung von Klonvorgängen für SAP HANA Datenbanken 326
Teilen Sie einen Klon auf 326
Löschen oder teilen Sie SAP HANA Datenbankklone nach dem Upgrade der SnapCenter 328

Schutz von Oracle Datenbanken . . . 329
Überblick über das SnapCenter Plug-in für Oracle Database . . . 329
Welche Möglichkeiten bietet das Plug-in für Oracle Database . . . 329
Funktionen von Plug-in für Oracle Database . . . 329
Von Plug-in für Oracle Database unterstützte Storage-Typen . . . 331
Storage-Systeme für SnapMirror und SnapVault Replizierung für Plug-in für Oracle vorbereiten . . . 333
Minimale ONTAP-Berechtigungen, die für das Plug-in für Oracle erforderlich sind . . . 333
Installieren Sie das SnapCenter Plug-in für Oracle Database . . . 335
Installations-Workflow des SnapCenter Plug-ins für Oracle Database . . . 336
Voraussetzungen für das Hinzufügen von Hosts und die Installation von Plug-ins Package für Linux oder AIX . . . 336
Fügen Sie Hosts hinzu und installieren Sie mithilfe der GUI das Plug-ins Package für Linux oder AIX . . . 345
Alternative Möglichkeiten, Plug-ins Package für Linux oder AIX zu installieren . . . 350
Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst . . . 353
Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Service auf dem Linux-Host . . . 356
Aktivieren Sie CA-Zertifikate für Plug-ins . . . 359
Import der Daten von SnapManager für Oracle und SnapManager für SAP zu SnapCenter . . . 360
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 366
Bereitstellen eines CA-Zertifikats . . . 366
Konfigurieren Sie die CRL-Datei . . . 366
Bereiten Sie sich auf den Schutz von Oracle Datenbanken vor . . . 366
Backup von Oracle Datenbanken . . . 368
Überblick über den Sicherungsvorgang . . . 368
Konfigurationsinformationen sichern . . . 369
Anforderungen für das Backup einer Oracle-Datenbank . . . 381
Entdecken Sie die für Backups verfügbaren Oracle-Datenbanken . . . 382
Erstellung von Backup-Richtlinien für Oracle Datenbanken . . . 384
Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Oracle-Datenbanken . . . 390
Oracle-Ressourcen sichern . . . 392
Sichern Sie Oracle Database Resource Groups . . . 395
Überwachen Sie das Backup von Oracle Datenbanken . . . 396
Andere Backup-Vorgänge . . . 397
Binden Sie Datenbank-Backups ein und heben Sie sie ab . . . 402
Mounten Sie ein Datenbank-Backup . . . 402
Heben Sie die Bereitstellung eines Datenbank-Backups auf . . . 404
Stellen Sie Oracle Datenbanken wieder her . . . 404
Wiederherstellung des Workflows . . . 404
Definition einer Restore- und Recovery-Strategie für Oracle Datenbanken . . . 404
Vordefinierte Umgebungsvariablen zur Wiederherstellung spezifischer Vorschrift und Postscript . . . 409
Anforderungen für die Wiederherstellung einer Oracle-Datenbank . . . 411
Stellen Sie Oracle Datenbanken wieder her . . . 412
Wiederherstellen von Tabellen mit Point-in-Time Recovery . . . 417
Wiederherstellen steckbarer Datenbanken über zeitpunktgenaues Recovery . . . 419
Stellen Sie Oracle Datenbanken mithilfe von UNIX-Befehlen wieder her . . . 421

Überwachen Sie die Restore-Vorgänge für Oracle Datenbanken . . . 422
Wiederherstellungsvorgänge für Oracle-Datenbank abbrechen . . . 423
Oracle Datenbank klonen . . . 423
Klon-Workflow . . . 423
Klonstrategie für Oracle Datenbanken definieren . . . 424
Vordefinierte Umgebungsvariablen für das Klonen spezifischer Prescript und Postscript . . . 425
Anforderungen für das Klonen einer Oracle Datenbank . . . 427
Klonen eines Backups einer Oracle Datenbank . . . 429
Klonen einer sofort anschließbaren Datenbank . . . 438
Backups der Oracle Datenbank mit UNIX Befehlen klonen . . . 443
Oracle Database klonen . . . 443
Split-Klon einer steckbaren Datenbank . . . 444
Überwachen Sie die Klonvorgänge von Oracle Datenbanken . . . 445
Aktualisieren Sie einen Klon . . . 446
Löschen des Klons einer steckbaren Datenbank . . . 447
Management von Applikations-Volumes . . . 447
Was sind Applikations-Volumes . . . 447
Hinzufügen von Applikations-Volumes . . . 448
Backup-Anwendungsvolumes . . . 449
Backup von Klon-Applikations-Volumes . . . 451
Sichern Sie Windows Filesysteme . . . 454
SnapCenter Plug-in für Microsoft Windows-Konzepte . . . 454
SnapCenter Plug-in für Microsoft Windows – Übersicht . . . 454
Was Sie mit dem SnapCenter Plug-in für Microsoft Windows tun können . . . 454
SnapCenter Plug-in für Windows Funktionen . . . 454
Wie SnapCenter Windows File-Systeme sichert . . . 455
Vom SnapCenter-Plug-in für Microsoft Windows unterstützte Storage-Typen . . . 456
Minimale ONTAP-Berechtigungen für Windows Plug-in erforderlich . . . 458
Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten . . . 461
Definieren einer Backup-Strategie für Windows File-Systeme . . . 461
Quellen und Ziele von Klonen für Windows Filesysteme . . . 463
Installieren Sie das SnapCenter Plug-in für Microsoft Windows . . . 463
Installationsworkflow des SnapCenter Plug-ins für Microsoft Windows . . . 464
Installationsanforderungen für das SnapCenter Plug-in für Microsoft Windows . . . 464
Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows . . . 469
Installieren Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Remote Hosts mithilfe von PowerShell cmdlets . . . 473
Installieren Sie das SnapCenter-Plug-in für Microsoft Windows im Hintergrund über die Befehlszeile . . . 473
Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets . . . 475
Konfigurieren Sie das CA-Zertifikat . . . 476
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 479
Bereitstellen eines CA-Zertifikats . . . 479
Konfigurieren Sie die CRL-Datei . . . 479
Sichern Sie Windows File-Systeme . . . 480
Sichern Sie Windows File-Systeme . . . 480

Bestimmen Sie die Verfügbarkeit von Ressourcen für Windows File-Systeme . . . 480
Erstellen von Backup-Richtlinien für Windows Filesysteme . . . 481
Erstellen von Ressourcengruppen für Windows-Dateisysteme . . . 485
Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets . . . 488
Bedarfsgerechtes Backup für eine einzelne Ressource für Windows File-Systeme . . . 489
Sichern Sie Ressourcengruppen für Windows File-Systeme . . . 493
Monitoring von Backup-Vorgängen . . . 494
Abbrechen von Backup-Vorgängen . . . 495
Sehen Sie sich zugehörige Backups und Klone auf der Seite Topologie an . . . 496
Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets . . . 499
Stellen Sie Windows-Dateisysteme wieder her . . . 499
Windows Dateisystemsicherungen wiederherstellen . . . 499
Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her . . . 504
Überwachen von Restore-Vorgängen . . . 507
Wiederherstellungsvorgänge abbrechen . . . 508
Klonen von Windows Filesystemen . . . 509
Klonen aus einem Windows File-System-Backup . . . 509
Monitoring von Klonvorgängen . . . 515
Klonvorgänge abbrechen . . . 516
Teilen Sie einen Klon auf . . . 517
Schutz von Microsoft Exchange Server Datenbanken . . . 519
SnapCenter Plug-in für Microsoft Exchange Server-Konzepte . . . 519
Übersicht über das SnapCenter Plug-in für Microsoft Exchange Server . . . 519
Ihre Möglichkeiten mit dem SnapCenter Plug-in für Microsoft Exchange Server . . . 519
Storage-Typen, die von SnapCenter Plug-in für Microsoft Windows und für Microsoft Exchange Server unterstützt werden . . . 520
Minimale ONTAP-Berechtigungen, die für das Exchange Plug-in erforderlich sind . . . 521
Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten . . . 524
Backup-Strategie für Exchange Server-Ressourcen definieren . . . 524
Festlegen einer Restore-Strategie für Exchange-Datenbanken . . . 527
Installieren Sie das SnapCenter Plug-in für Microsoft Exchange Server . . . 528
Installations-Workflow des SnapCenter Plug-ins für Microsoft Exchange Server . . . 528
Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter Plug-ins für Microsoft Exchange Server . . . 529
Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-in für Windows ein . . . 533
Konfigurieren Sie gMSA unter Windows Server 2016 oder höher . . . 534
Fügen Sie Hosts hinzu und installieren Sie das Plug-in für Exchange . . . 536
Installieren Sie das Plug-in für Exchange über den SnapCenter Server Host mithilfe von PowerShell Cmdlets . . . 542
Installieren Sie das SnapCenter Plug-in für Exchange im Hintergrund über die Befehlszeile . . . 543
Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets . . . 544
Konfigurieren Sie das CA-Zertifikat . . . 545
Konfigurieren Sie SnapManager 7.x für Exchange und SnapCenter, um koexistieren zu können . . . 548
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 550
Bereitstellen eines CA-Zertifikats . . . 550

Konfigurieren Sie die CRL-Datei . . . 550
Bereiten Sie sich auf die Datensicherung vor . . . 551
Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für Microsoft Exchange Server . . . 551
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von Exchange Server verwendet werden . . . 552
Exchange-Ressourcen sichern . . . 553
Backup-Workflow . . . 553
Exchange Datenbank und Backup-Verifizierung . . . 554
Bestimmen Sie, ob Exchange Ressourcen für Backups verfügbar sind . . . 554
Erstellen von Backup-Richtlinien für Exchange Server-Datenbanken . . . 556
Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Exchange-Server . . . 563
Erstellen Sie eine Storage-Systemverbindung und Zugangsdaten mit PowerShell cmdlets für Exchange Server . . . 566
Backup von Exchange Datenbanken . . . 567
Sichern von Exchange-Ressourcengruppen . . . 573
Monitoring von Backup-Vorgängen . . . 574
Abbrechen der Backup-Vorgänge für die Exchange-Datenbank . . . 575
Zeigen Sie Exchange-Backups auf der Seite Topologie an . . . 576
Stellen Sie Exchange Ressourcen wieder her . . . 578
Wiederherstellung des Workflows . . . 578
Anforderungen für die Wiederherstellung einer Exchange-Datenbank . . . 578
Exchange Datenbanken wiederherstellen . . . 579
Granulares Recovery von Mails und Mailboxen . . . 583
Wiederherstellung einer Exchange Server-Datenbank aus dem sekundären Storage . . . 583
Erneutes Seeding eines passiven Exchange Node-Replikats . . . 584
Erneutes Seeding mit PowerShell cmdlets für Exchange Datenbank . . . 585
Überwachen von Restore-Vorgängen . . . 586
Abbrechen von Wiederherstellungsvorgängen für Exchange-Datenbank . . . 586
Schutz von IBM DB2 . . . 588
SnapCenter Plug-in für IBM DB2 . . . 588
Übersicht über das SnapCenter Plug-in für IBM DB2 . . . 588
Was Sie mit dem SnapCenter-Plug-in für IBM DB2 tun können . . . 588
Funktionen des SnapCenter Plug-ins für IBM DB2 . . . 589
Vom SnapCenter-Plug-in für IBM DB2 unterstützte Storage-Typen . . . 589
Für das IBM DB2-Plug-in sind minimale ONTAP-Berechtigungen erforderlich . . . 590
Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replizierung für IBM DB2 vor . . . 593
Backup-Strategie für IBM DB2 . . . 593
Restore- und Recovery-Strategie für IBM DB2 . . . 596
Bereiten Sie die Installation des SnapCenter-Plug-ins für IBM DB2 vor . . . 597
Installationsworkflow des SnapCenter-Plug-ins für IBM DB2 . . . 597
Voraussetzungen für das Hinzufügen von Hosts und das Installieren des Plug-ins-Pakets für Windows, Linux oder AIX . . . 597
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows . . . 603
Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux . . . 604
Anmeldedaten für das SnapCenter-Plug-in für IBM DB2 einrichten . . . 604

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher . . . 607
Installieren Sie das SnapCenter-Plug-in für IBM DB2 . . . 608
Konfigurieren Sie das CA-Zertifikat . . . 614
Bereiten Sie sich auf die Datensicherung vor . . . 623
Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für IBM DB2 . . . 623
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von IBM DB2 verwendet werden . . . 623
Backup von IBM DB2-Ressourcen . . . 624
Backup von IBM DB2-Ressourcen . . . 624
Automatische Erkennung von Datenbanken . . . 626
Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu . . . 626
Backup-Richtlinien für IBM DB2 erstellen . . . 628
Erstellen von Ressourcengruppen und Anhängen von Richtlinien . . . 629
Erstellen Sie mit PowerShell-Cmdlets für IBM DB2 eine Verbindung zum Speichersystem und Zugangsdaten . . . 633
Backup von DB2-Datenbanken . . . 635
Sichern von Ressourcengruppen . . . 642
Überwachung von IBM DB2 Backup-Vorgängen . . . 643
Abbrechen von Backup-Vorgängen für IBM DB2 . . . 644
Zeigen Sie IBM DB2-Backups und -Klone auf der Topology-Seite an . . . 645
Stellen Sie IBM DB2 wieder her . . . 647
Wiederherstellung des Workflows . . . 647
Stellen Sie ein manuell hinzugefügtes Ressourcenbackup wieder her . . . 647
Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her . . . 652
Überwachung der IBM DB2-Wiederherstellungsvorgänge . . . 654
Klonen Sie IBM DB2-Ressourcen-Backups . . . 654
Klon-Workflow . . . 655
Klonen eines IBM DB2 Backups . . . 655
Überwachung von IBM DB2-Klonvorgängen . . . 662
Teilen Sie einen Klon auf . . . 663
Löschen oder teilen Sie IBM DB2 Datenbankklone nach dem Upgrade von SnapCenter . . . 664
Schützen Sie PostgreSQL . . . 666
SnapCenter Plug-in für PostgreSQL . . . 666
Übersicht über das SnapCenter Plug-in für PostgreSQL . . . 666
Was Sie mit dem SnapCenter Plug-in für PostgreSQL tun können . . . 666
Funktionen des SnapCenter Plug-in für PostgreSQL . . . 666
Von SnapCenter Plug-in für PostgreSQL unterstützte Speichertypen . . . 667
Für das PostgreSQL-Plug-in sind mindestens ONTAP-Berechtigungen erforderlich . . . 668
Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replication für PostgreSQL vor . . . 671
Backup-Strategie für PostgreSQL . . . 671
Restore- und Recovery-Strategie für PostgreSQL . . . 674
Bereiten Sie die Installation des SnapCenter-Plug-ins für PostgreSQL vor . . . 675
Installationsworkflow des SnapCenter Plug-in für PostgreSQL . . . 675
Voraussetzungen, um Hosts hinzuzufügen und das SnapCenter-Plug-in für PostgreSQL zu installieren . . . 676
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows . . . 679

Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux . . . 680
Anmeldedaten für das SnapCenter-Plug-in für PostgreSQL einrichten . . . 681
Konfigurieren Sie gMSA unter Windows Server 2016 oder höher . . . 684
Installieren Sie das SnapCenter-Plug-in für PostgreSQL . . . 685
Konfigurieren Sie das CA-Zertifikat . . . 691
Bereiten Sie sich auf die Datensicherung vor . . . 700
Voraussetzungen für die Verwendung des SnapCenter Plug-ins für PostgreSQL . . . 700
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von PostgreSQL verwendet werden . . . 700
Sichern Sie PostgreSQL-Ressourcen . . . 701
Sichern Sie PostgreSQL-Ressourcen . . . 701
Automatische Erkennung der Cluster . . . 703
Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu . . . 703
Erstellen Sie Backup-Richtlinien für PostgreSQL . . . 705
Erstellen von Ressourcengruppen und Anhängen von Richtlinien . . . 707
Erstellen Sie mit PowerShell Cmdlets für PostgreSQL eine Verbindung zum Speichersystem und Zugangsdaten . . . 711
Sichern Sie PostgreSQL . . . 713
Sichern von Ressourcengruppen . . . 718
Überwachen von PostgreSQL-Backup-Vorgängen . . . 719
Backup-Vorgänge für PostgreSQL abbrechen . . . 720
Zeigen Sie PostgreSQL-Backups und Clones auf der Seite Topologie an . . . 721
PostgreSQL wiederherstellen . . . 723
Wiederherstellung des Workflows . . . 723
Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups . . . 723
Wiederherstellung und Wiederherstellung einer automatisch erkannten Cluster-Sicherung . . . 728
Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her . . . 731
Überwachen Sie die PostgreSQL-Wiederherstellungsvorgänge . . . 733
Klonen von PostgreSQL-Ressourcen-Backups . . . 734
Klon-Workflow . . . 734
Klonen eines PostgreSQL-Backups . . . 735
Überwachen von PostgreSQL-Klonvorgängen . . . 738
Teilen Sie einen Klon auf . . . 739
Löschen oder teilen Sie PostgreSQL Cluster Clones nach dem Upgrade von SnapCenter . . . 740
MySQL schützen . . . 742
SnapCenter Plug-in für MySQL . . . 742
Übersicht über das SnapCenter Plug-in für MySQL . . . 742
Was Sie mit dem SnapCenter-Plug-in für MySQL tun können . . . 742
SnapCenter Plug-in für MySQL Funktionen . . . 742
Vom SnapCenter-Plug-in für MySQL unterstützte Storage-Typen . . . 743
Für das MySQL Plug-in sind minimale ONTAP-Berechtigungen erforderlich . . . 744
Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replizierung für MySQL vor . . . 747
Backup-Strategie für MySQL . . . 747
Restore- und Recovery-Strategie für MySQL . . . 750
Bereiten Sie die Installation des SnapCenter-Plug-ins für MySQL vor . . . 751

Installationsworkflow des SnapCenter Plug-ins für MySQL . . . 751
Voraussetzungen, um Hosts hinzuzufügen und das SnapCenter-Plug-in für MySQL zu installieren . . . 751
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows . . . 755
Host-Anforderungen für die Installation des SnapCenter Plug-ins Pakets für Linux . . . 756
Anmeldedaten für das SnapCenter-Plug-in für MySQL einrichten . . . 757
Installieren Sie das SnapCenter-Plug-in für MySQL . . . 760
Konfigurieren Sie das CA-Zertifikat . . . 765
Bereiten Sie sich auf die Datensicherung vor . . . 773
Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für MySQL . . . 773
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von MySQL verwendet werden . . . 774
Backup von MySQL Ressourcen . . . 774
Backup von MySQL Ressourcen . . . 774
Automatische Erkennung von Datenbanken . . . 776
Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu . . . 776
Backup-Richtlinien für MySQL erstellen . . . 778
Erstellen von Ressourcengruppen und Anhängen von Richtlinien . . . 779
Erstellen Sie eine Storage-Systemverbindung und Zugangsdaten mit PowerShell Cmdlets für MySQL . . . 783
Backup von MySQL . . . 785
Sichern von Ressourcengruppen . . . 790
Monitoring von MySQL Backup-Vorgängen . . . 791
Backup-Vorgänge für MySQL abbrechen . . . 792
Zeigen Sie MySQL-Backups und -Klone auf der Seite Topologie an . . . 793
Stellen Sie MySQL wieder her . . . 795
Wiederherstellung des Workflows . . . 795
Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups . . . 795
Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her . . . 800
Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her . . . 802
Überwachen von MySQL-Wiederherstellungsvorgängen . . . 804
Klonen von MySQL-Ressourcen-Backups . . . 805
Klon-Workflow . . . 805
Klonen eines MySQL-Backups . . . 806
Überwachen von MySQL-Klonvorgängen . . . 809
Teilen Sie einen Klon auf . . . 810
Löschen oder teilen Sie MySQL-Datenbankklone nach dem Upgrade von SnapCenter . . . 811
Schützen Sie Applikationen mit von NetApp unterstützten Plug-ins . . . 813
Von NetApp unterstützte Plug-ins . . . 813
Übersicht über die unterstützten Plug-ins von NetApp . . . 813
Funktionen der von NetApp unterstützten Plug-ins . . . 813
Von NetApp unterstützte Plug-ins-Funktionen . . . 814
Von von NetApp unterstützte Plug-ins unterstützte Storage-Typen . . . 815
Minimale ONTAP-Berechtigungen für von NetApp unterstütztes Plug-in erforderlich . . . 815
Vorbereiten der Storage-Systeme für die SnapMirror und SnapVault Replizierung für von NetApp unterstützte Plug-ins . . . 817
Backup-Strategie definieren . . . 818
Backup-Strategie für von NetApp unterstützte Plug-ins . . . 819

Typen von Wiederherstellungsstrategien, die für manuell hinzugefügte NetApp-unterstützte Plug-in-Ressourcen unterstützt werden . . . 820
Bereiten Sie die Installation von NetApp-unterstützten Plug-ins vor . . . 820
Installations-Workflow von von SnapCenter NetApp unterstützten Plug-ins . . . 820
Voraussetzungen für das Hinzufügen von Hosts und das Installieren des Plug-ins-Pakets für Windows, Linux oder AIX . . . 821
Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows . . . 825
Host-Anforderungen für die Installation des SnapCenter-Plug-ins-Pakets für Linux und AIX . . . 826
Richten Sie Anmeldeinformationen für von NetApp unterstützte Plug-ins ein . . . 827
Konfigurieren Sie gMSA unter Windows Server 2016 oder höher . . . 830
Installieren Sie die von NetApp unterstützten Plug-ins . . . 831
Konfigurieren Sie das CA-Zertifikat . . . 838
Bereiten Sie sich auf die Datensicherung vor . . . 846
Voraussetzungen für die Verwendung der von NetApp unterstützten Plug-ins . . . 846
Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von von NetApp unterstützten Plug-in-Ressourcen verwendet werden . . . 847
Backup von von NetApp unterstützten Plug-ins-Ressourcen . . . 848
Backup von von NetApp unterstützten Plug-ins-Ressourcen . . . 848
Hinzufügen von Ressourcen zu von NetApp unterstützten Plug-ins . . . 848
Erstellen von Richtlinien für von NetApp unterstützte Plug-in-Ressourcen . . . 853
Erstellen von Ressourcengruppen und Anhängen von Richtlinien . . . 858
Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets . . . 861
Backup einzelner von NetApp unterstützter Plug-ins-Ressourcen . . . 862
Backup von Ressourcengruppen von von NetApp unterstützten Plug-in-Ressourcen . . . 868
Überwachung von Backup-Vorgängen bei von NetApp unterstützten Plug-in-Ressourcen . . . 869
Abbrechen von Backup-Vorgängen für von NetApp unterstützte Plug-ins . . . 870
Zeigen Sie auf der Seite „Topologie“ ressourcenbezogene Backups und Klone von NetApp-unterstützten Plug-ins an . . . 871
Stellen Sie von NetApp unterstützte Plug-ins-Ressourcen wieder her . . . 873
Stellen Sie von NetApp unterstützte Plug-in-Ressourcen wieder her . . . 873
Wiederherstellen eines Ressourcenbackups . . . 873
Überwachen von Wiederherstellungsvorgängen mit von NetApp unterstützten Plug-in-Ressourcen . . . 878
Von NetApp unterstütztes Klon-Plug-in-Ressourcen-Backups . . . 879
Von NetApp unterstütztes Klon-Plug-in-Ressourcen-Backups . . . 879
Klonen aus einem Backup . . . 880
Überwachen von von NetApp unterstützten Plug-in-Ressourcenklonoperationen . . . 886
Schützen Sie Unix-Dateisysteme . . . 888
Was Sie mit dem SnapCenter-Plug-in für Unix-Dateisysteme tun können . . . 888
Unterstützte Konfigurationen . . . 888
Einschränkungen . . . 889
Installieren Sie das SnapCenter-Plug-in für Unix-Dateisysteme . . . 889
Voraussetzungen für das Hinzufügen von Hosts und das Installieren von Plug-ins Package für Linux . . . 889
Fügen Sie Hosts hinzu und installieren Sie Plug-ins Package for Linux mithilfe der GUI . . . 890
Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst . . . 893
Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Service auf dem Linux-

Host . . . 897
Aktivieren Sie CA-Zertifikate für Plug-ins . . . 900
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 900
Bereitstellen eines CA-Zertifikats . . . 900
Konfigurieren Sie die CRL-Datei . . . 901
Bereiten Sie sich auf den Schutz von Unix-Dateisystemen vor . . . 901
Sichern Sie Unix-Dateisysteme . . . 901
Ermitteln Sie die für Backups verfügbaren UNIX-Dateisysteme . . . 901
Erstellen Sie Backup-Richtlinien für Unix-Dateisysteme . . . 902
Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Unix-Dateisysteme . . . 905
Sichern Sie Unix-Dateisysteme . . . 907
Erstellen Sie ein Backup von Ressourcengruppen für Unix-Dateisysteme . . . 908
Überwachen Sie das Backup von Unix-Dateisystemen . . . 909
Zeigen Sie geschützte Unix-Dateisysteme auf der Seite Topologie an . . . 910
Stellen Sie Unix-Dateisysteme wieder her . . . 913
Stellen Sie Unix-Dateisysteme wieder her . . . 913
Überwachen Sie die Wiederherstellungsvorgänge von Unix-Dateisystemen . . . 915
Klonen von Unix-Dateisystemen . . . 915
Klonen des Unix Filesystem-Backups . . . 915
Teilen Sie einen Klon auf . . . 917
Überwachen Sie die Klonvorgänge von Unix-Dateisystemen . . . 918
Sichern Sie Applikationen, die auf Azure NetApp Files ausgeführt werden . . . 920
Sichern Sie Applikationen, die auf Azure NetApp Files ausgeführt werden . . . 920
Einschränkungen . . . 920
Installieren Sie SnapCenter und erstellen Sie Anmeldeinformationen . . . 920
Installieren Sie SnapCenter auf der Azure Virtual Machine . . . 920
Erstellen Sie die Azure-Zugangsdaten in SnapCenter . . . 922
Konfigurieren Sie das Azure Storage-Konto . . . 922
Erstellen Sie die Anmeldeinformationen, um den Plug-in-Host hinzuzufügen . . . 923
Schutz von SAP HANA Datenbanken . . . 924
Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die SAP HANA Datenbank . . . 924
Fügen Sie die SAP HANA-Datenbank hinzu . . . 924
Backup-Richtlinien für SAP HANA Datenbanken . . . 925
Ressourcengruppen erstellen und SAP HANA Backup-Richtlinien anhängen . . . 926
Sichern Sie auf Azure NetApp Files ausgeführte SAP HANA-Datenbanken . . . 927
Backup von SAP HANA-Ressourcengruppen . . . 928
Wiederherstellung von SAP HANA Datenbanken . . . 928
Klonen des SAP HANA Datenbank-Backups . . . 929
Microsoft SQL Server Datenbanken schützen . . . 930
Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die SQL Server-Datenbank . . . 930
Erstellen von Backup-Richtlinien für SQL Server-Datenbanken . . . 931
Erstellen von Ressourcengruppen und Anhängen von SQL-Backup-Richtlinien . . . 932
Sichern Sie auf Azure NetApp Files laufende SQL Server Datenbanken . . . 934
Sichern Sie SQL Server-Ressourcengruppen . . . 935
Stellen Sie SQL Server Datenbanken wieder her . . . 935

Klonen Sie das SQL Server Datenbank-Backup . . . 936
Schutz von Oracle Datenbanken . . . 938
Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank . . . 938
Erstellung von Backup-Richtlinien für Oracle Datenbanken . . . 939
Erstellen von Ressourcengruppen und Anhängen von Oracle-Backup-Richtlinien . . . 940
Sichern Sie auf Azure NetApp Files laufende Oracle Datenbanken . . . 941
Erstellen Sie ein Backup von Oracle Ressourcengruppen . . . 942
Stellen Sie Oracle Datenbanken wieder her . . . 942
Klonen Sie das Backup von Oracle Datenbanken . . . 945
Management von SnapCenter Server und Plug-ins . . . 948
Dashboard anzeigen . . . 948
Überblick über das Dashboard . . . 948
So zeigen Sie Informationen auf dem Dashboard an . . . 952
Statusberichte der Jobs über das Dashboard anfordern . . . 952
Berichte zum Sicherungsstatus können über das Dashboard angefordert werden . . . 953
RBAC managen . . . 954
Ändern Sie eine Rolle . . . 954
Benutzer und Gruppen ändern . . . 954
Management von Hosts . . . 955
Informationen zu Virtual Machines aktualisieren . . . 957
Ändern Sie die Plug-in-Hosts . . . 957
Plug-in-Dienste starten oder neu starten . . . 958
Unterbrechen Sie die Zeitpläne für die Hostwartung . . . 958
Von der Seite Ressourcen unterstützte Vorgänge . . . 959
Management von Richtlinien . . . 960
Richtlinien ändern . . . 960
Richtlinien trennen . . . 961
Richtlinien löschen . . . 961
Verwalten von Ressourcengruppen . . . 962
Stoppen und fortsetzen Sie den Betrieb in Ressourcengruppen . . . 962
Löschen von Ressourcengruppen . . . 963
Backup-Management . . . 963
Backups umbenennen . . . 963
Backups löschen . . . 964
Schutz entfernen . . . 964
Klone löschen . . . 965
Überwachen von Jobs, Zeitplänen, Ereignissen und Protokollen . . . 966
Überwachen von Jobs . . . 966
Überwachung von Zeitplänen . . . 967
Monitoring von Ereignissen . . . 967
Monitoring von Protokollen . . . 968
Entfernen Sie Jobs und Protokolle aus SnapCenter . . . 969
Überblick über die Berichterstellungsfunktionen von SnapCenter . . . 969
Aufrufen von Berichten . . . 971
Filtern Sie Ihren Bericht . . . 971

Berichte exportieren oder drucken . . . 972
Stellen Sie den SMTP-Server für E-Mail-Benachrichtigungen ein . . . 972
Konfigurieren Sie die Option zum E-Mail-Versenden von Berichten . . . 972
Verwalten des SnapCenter-Server-Repositorys . . . 973
Voraussetzungen für den Schutz des SnapCenter-Repositorys . . . 973
Sichern des SnapCenter Repositorys . . . 973
Anzeigen von Backups des SnapCenter Repositorys . . . 974
Wiederherstellung des SnapCenter Datenbank-Repositorys . . . 974
SnapCenter-Repository migrieren . . . 975
Setzen Sie das SnapCenter Repository-Kennwort zurück . . . 975
Management von Ressourcen von nicht vertrauenswürdigen Domänen . . . 976
Ändern Sie nicht vertrauenswürdige Domains . . . 976
Nicht vertrauenswürdige Active Directory-Domänen werden nicht registriert . . . 977
Management des Storage-Systems . . . 978
Konfiguration des Storage-Systems ändern . . . 978
Löschen Sie das Speichersystem . . . 980
EMS-Datenerfassung managen . . . 981
EMS-Datenerfassung stoppen . . . 981
Starten Sie die EMS-Datensammlung . . . 981
EMS-Datenerfassungsplan und Ziel-SVM ändern . . . 981
Den EMS-Datenerfassungsstatus überwachen . . . 982
Aktualisieren Sie SnapCenter Server und Plug-ins . . . 983
Konfigurieren Sie SnapCenter, um nach verfügbaren Updates zu suchen . . . 983
Workflow-Upgrade . . . 983
Unterstützte Upgrade-Pfade . . . 983
Aktualisieren Sie den SnapCenter-Server auf dem Windows-Host . . . 984
Aktualisieren Sie den SnapCenter-Server auf dem Linux-Host . . . 986
Aktualisieren Sie Ihre Plug-in-Pakete . . . 987
Technologieaktualisierung . . . 990
Technologieaktualisierung des SnapCenter-Serverhosts . . . 990
Tech Refresh eines Node in F5 Cluster . . . 991
Den alten SnapCenter-Server-Host stilllegen . . . 991
Rollback auf den alten SnapCenter-Server-Host durchführen . . . 991
Disaster Recovery . . . 991
Technologieaktualisierung bei SnapCenter Plug-in-Hosts . . . 993
Technologieaktualisierung des Storage-Systems . . . 996
Aktualisieren Sie die Backups des primären Speichers . . . 996
Aktualisieren Sie die Backups des sekundären Speichers . . . 998
Deinstallieren Sie SnapCenter Server und Plug-ins . . . 1000
Deinstallieren Sie SnapCenter-Plug-in-Pakete . . . 1000
Voraussetzungen für das Entfernen eines Hosts . . . 1000
Entfernen Sie einen Host . . . 1001
Deinstallieren Sie Plug-ins über die SnapCenter-GUI . . . 1001
Deinstallieren Sie Windows Plug-ins mit dem PowerShell Cmdlet . . . 1002
Deinstallieren Sie Plug-ins lokal auf einem Host . . . 1003

Deinstallieren Sie das Plug-ins-Paket für Linux oder AIX mithilfe von CLI . . . 1004
Deinstallieren Sie den SnapCenter-Server auf dem Windows-Host . . . 1004
Deinstallieren Sie den SnapCenter-Server auf dem Linux-Host . . . 1005
Automatisierung mit REST-APIs . . . 1006
Übersicht ÜBER REST-APIs . . . 1006
Wie kann man nativ auf die SnapCenter REST-API zugreifen . . . 1006
REST-Web-Services-Grundlage . . . 1006
Ressourcen- und Zustandsdarstellung . . . 1006
URI-Endpunkte . . . 1007
HTTP-Meldungen . . . 1007
JSON-Formatierung . . . 1007
Grundlegende betriebliche Eigenschaften . . . 1007
API-Transaktion bei Anfrage und Reaktion . . . 1007
Unterstützung von CRUD-Vorgängen . . . 1007
Objektkennungen . . . 1008
Objektinstanzen und -Sammlungen . . . 1008
Synchroner und asynchroner Betrieb . . . 1008
Sicherheit . . . 1008
Eingabevariablen, die eine API-Anforderung steuern . . . 1009
HTTP-Methoden . . . 1009
Anfragekopfzeilen . . . 1009
Text anfordern . . . 1010
Objekte filtern . . . 1010
Es werden bestimmte Objektfelder angefordert . . . 1010
Sortieren von Objekten im Ausgabungsset . . . 1011
Paginierung beim Abrufen von Objekten in einer Sammlung . . . 1011
Größeneigenschaften . . . 1012
Interpretation einer API-Antwort . . . 1012
HTTP-Statuscode . . . 1013
Antwortkopfzeilen . . . 1013
Antwortkörper . . . 1013
Fehler . . . 1014
REST-APIs werden für SnapCenter Server und Plug-ins unterstützt . . . 1015
Auth . . . 1015
Domänen . . . 1015
Jobs . . . 1015
Einstellungen . . . 1015
Hosts . . . 1016
Ressourcen . . . 1016
Backups . . . 1018
Klone . . . 1018
Aufteilung klonen . . . 1019
Ressourcengruppen . . . 1019
Richtlinien . . . 1019
Storage . . . 1019

Share . . . 1020
Plug-Ins . . . 1020
Berichte An . . . 1021
Meldungen . . . 1021
Rbac . . . 1021
Konfiguration . . . 1022
Zertifikateinstellungen . . . 1022
Repository . . . 1022
Version . . . 1022
Zugriff auf REST-APIs über die Swagger API-Webseite . . . 1022
Legen Sie los mit DER REST API . . . 1023
Hallo Welt . . . 1023
Rechtliche Hinweise . . . 1024
Urheberrecht . . . 1024
Marken . . . 1024
Patente . . . 1024
Datenschutzrichtlinie . . . 1024
Open Source . . . 1024

SnapCenter-Softwaredokumentation

Versionshinweise

Versionshinweise

Erfahren Sie mehr über die neuen und erweiterten Funktionen in SnapCenter 6.0 und 6.0.1.

Eine vollständige Liste der neuen Funktionen und Verbesserungen finden Sie unter "Was ist neu in SnapCenter 6.0.1" und "Was ist neu in SnapCenter 6.0".

Details zu bekannten Problemen, Einschränkungen, behobene Probleme sowie zu neuen und geänderten Befehlen finden Sie im "Versionshinweise zu SnapCenter Software 6.0 und 6.0.1". Sie müssen sich mit Ihrem NetApp Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zuzugreifen.

Unterstützte Upgrade-Pfade für SnapCenter

Der Upgrade-Pfad verhilft Ihnen zu einem Bild davon, von welchen älteren SnapCenter Versionen Sie ein Upgrade auf die neueste SnapCenter Version durchführen können und welche Plug-ins-Versionen unterstützt werden.

Wenn Sie sich auf SnapCenter Server-Version befinden…	Sie können ein Upgrade des SnapCenter-Servers direkt auf…	Unterstützte Plug-in-Versionen
4,9	5,0	• 4,9 • 5,0
	6,0	• 6,0
5,0	6,0	• 5,0 • 6,0
	6.0.1	• 6.0.1
6,0	6.0.1	• 6,0 • 6.0.1

Wenn Sie beispielsweise SnapCenter Version 4.9 verwenden und auf 6.0 aktualisieren möchten, sollten Sie zuerst ein Upgrade auf 5.0 durchführen und dann ein Rolling Upgrade auf 6.0 durchführen.

Informationen zum Upgrade des SnapCenter-Plug-ins für VMware vSphere finden Sie unter "Aktualisieren Sie das SnapCenter Plug-in für VMware vSphere".

Konzepte

Übersicht über SnapCenter

SnapCenter Software ist eine einfache, zentralisierte und skalierbare Plattform, die applikationskonsistenten Datenschutz für Applikationen, Datenbanken, Host-Filesysteme und VMs bietet, die auf ONTAP Systemen in der Hybrid Cloud ausgeführt werden.

SnapCenter bietet mithilfe von NetApp Snapshot, SnapRestore, FlexClone, SnapMirror und SnapVault Technologien folgende Vorteile:

- Schnelle, platzsparende, applikationskonsistente festplattenbasierte Backups
- Rasante, granulare Wiederherstellung und applikationskonsistente Recoverys
- Schnelles, platzsparendes Klonen

SnapCenter enthält sowohl SnapCenter Server als auch individuelle schlanke Plug-ins. Sie können die Implementierung von Plug-ins für Remote-Applikations-Hosts automatisieren, Backup-, Verifizierungs- und Klonvorgänge planen und alle Datensicherungsvorgänge überwachen.

Es gibt folgende Möglichkeiten für die Implementierung von SnapCenter:

- Lokal, um Folgendes zu schützen:
  - Daten auf primären ONTAP FAS-, AFF- oder All-SAN-Array- (ASA) Systemen, die auf sekundäre ONTAP FAS-, AFF- oder ASA-Systeme repliziert werden
  - Daten auf primären ONTAP Select Systemen
  - Daten auf primären und sekundären ONTAP FAS, AFF oder ASA Systemen, die auf lokalem StorageGRID Objekt-Storage gesichert sind
- Lokal in einer Hybrid Cloud zur Sicherung folgender Komponenten:
  - Daten auf primären ONTAP FAS, AFF oder ASA Systemen, die auf Cloud Volumes ONTAP repliziert werden
  - Daten auf primären und sekundären ONTAP FAS-, AFF- oder ASA-Systemen, gesichert auf Objekt- und Archiv-Storage in der Cloud (mithilfe der BlueXP Backup- und Recovery-Integration)
- In einer Public Cloud zur Sicherung folgender Komponenten:
  - Daten auf primären Cloud Volumes ONTAP Systemen (früher ONTAP Cloud)
  - Daten auf Amazon FSX für ONTAP
  - Daten auf primärem Azure NetApp Files (Oracle, Microsoft SQL und SAP HANA)

SnapCenter umfasst folgende Kernfunktionen:

- Zentralisierte, applikationskonsistente Datensicherung

  Datensicherung wird für Microsoft Exchange Server, Microsoft SQL Server, Oracle Datenbanken auf Linux oder AIX, SAP HANA Datenbanken, IBM DB2, PostgreSQL, MySQL und Windows Host Dateisysteme auf ONTAP Systemen unterstützt. SnapCenter unterstützt auch den Schutz von Anwendungen wie MongoDB, Storage, MaxDB, Sybase ASE und ORASCPM.

- Richtlinienbasierte Backups

Richtlinienbasierte Backups nutzen die NetApp Snapshot Technologie, um schnelle, platzsparende, applikationskonsistente, festplattenbasierte Backups zu erstellen. Optional können Sie den Schutz dieser Backups auf dem sekundären Storage durch Updates vorhandener Sicherungsbeziehungen automatisieren.

- Backups mehrerer Ressourcen

  Sie können mehrere Ressourcen (Applikationen, Datenbanken oder Host-Filesysteme) desselben Typs gleichzeitig mithilfe von SnapCenter Ressourcengruppen sichern.

- Restore und Recovery

  SnapCenter ermöglicht schnelle, granulare Restores von Backups sowie applikationskonsistente, zeitbasierte Recoverys. Die Wiederherstellung ist von jedem Ziel in der Hybrid Cloud aus möglich.

- Klonen

  SnapCenter ermöglicht schnelles, platzsparendes, applikationskonsistentes Klonen und damit eine beschleunigte Software-Entwicklung. Sie können Klone auf jedem beliebigen Ziel in der Hybrid Cloud erstellen.

- Grafische Benutzeroberfläche (GUI) zum Einzelmanagement

  Die SnapCenter Benutzeroberfläche bietet eine einheitliche, zentrale Benutzeroberfläche für das Management von Backups und Klonen einer Ressource in jedem beliebigen Ziel in der Hybrid Cloud.

- REST-APIs, Windows Commandlets und UNIX Befehle

  SnapCenter umfasst REST-APIs für die meisten Funktionen zur Integration in jede Orchestrierungssoftware sowie die Verwendung von Windows PowerShell Cmdlets und Befehlszeilenschnittstelle.

  Weitere Informationen zu REST-APIs finden Sie unter "ÜBERSICHT ÜBER DIE REST-API".

  Weitere Informationen zu Windows-Cmdlets finden Sie unter "SnapCenter Software Cmdlet Referenzhandbuch".

  Weitere Informationen zu UNIX-Befehlen finden Sie unter "SnapCenter Software Command Reference Guide".

- Zentrale Datensicherungs-Konsole und Berichterstellung
- Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) für Sicherheit und Delegierung.
- Repository-Datenbank mit Hochverfügbarkeit

  SnapCenter bietet eine integrierte Repository-Datenbank mit Hochverfügbarkeit zum Speichern aller Backup-Metadaten.

- Automatisierte Push-Installation von Plug-ins

  Sie können einen Remote-Push von SnapCenter-Plug-ins vom SnapCenter Server Host an Applikations-Hosts automatisieren.

- Hochverfügbarkeit

  Hochverfügbarkeit für SnapCenter wird über externen Load Balancer (F5) eingerichtet. Im selben

Datacenter werden bis zu zwei Nodes unterstützt.

- Disaster Recovery (DR)

  Bei einem Ausfall wie z. B. einer Ressourcenbeschädigung oder einem Server-Absturz können Sie den SnapCenter Server wiederherstellen.

- SnapLock

  SnapLock ist eine hochperformante Compliance-Lösung für Unternehmen, die mit WORM-Storage (Write Once, Read Many) Dateien aus gesetzlichen und Governance-Gründen in unveränderter Form aufbewahren.

  Weitere Informationen zu SnapLock finden Sie unter "Was ist SnapLock"

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

  SnapMirror Active Sync ermöglicht Business Services auch bei einem vollständigen Standortausfall den Betrieb weiter und unterstützt Applikationen bei einem transparenten Failover mithilfe einer sekundären Kopie. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.

  Folgende Plug-ins werden für diese Funktion unterstützt: SnapCenter Plug-in für SQL Server, SnapCenter Plug-in für Windows, SnapCenter Plug-in für Oracle Database, SnapCenter Plug-in für SAP HANA Database, SnapCenter Plug-in für Microsoft Exchange Server und SnapCenter Plug-in für Unix.

  > Um die Nähe des Host-Initiators in SnapCenter zu unterstützen, sollte dieser Wert entweder als Quelle oder als Ziel in ONTAP festgelegt werden.

  Die SnapMirror Active Sync Funktion wird in SnapCenter nicht unterstützt:

  - Wenn Sie vorhandene asymmetrische SnapMirror Workloads mit aktiver Synchronisierung in symmetrisch konvertieren, indem Sie die Richtlinie für die aktiven SnapMirror Synchronisierungsbeziehungen von *automatisiertFailover* zu *automatisiertFailover* in ONTAP ändern, wird dies auch nicht in SnapCenter unterstützt.
  - Wenn Backups einer Ressourcengruppe (bereits in SnapCenter geschützt) vorhanden sind und dann die Storage-Richtlinie auf den aktiven Synchronisierungsbeziehungen von SnapMirror von *automatisiertFailover* auf *automatisiertFailover* in ONTAP geändert wird, wird dies auch nicht in SnapCenter unterstützt.

    Weitere Informationen zur aktiven SnapMirror Synchronisierung finden Sie unter "Übersicht über SnapMirror Active Sync"

  Stellen Sie für die aktive SnapMirror Synchronisierung sicher, dass Sie die verschiedenen Anforderungen an Hardware, Software und Systemkonfiguration erfüllt haben. Weitere Informationen finden Sie unter "Voraussetzungen"

- Synchrones Spiegeln

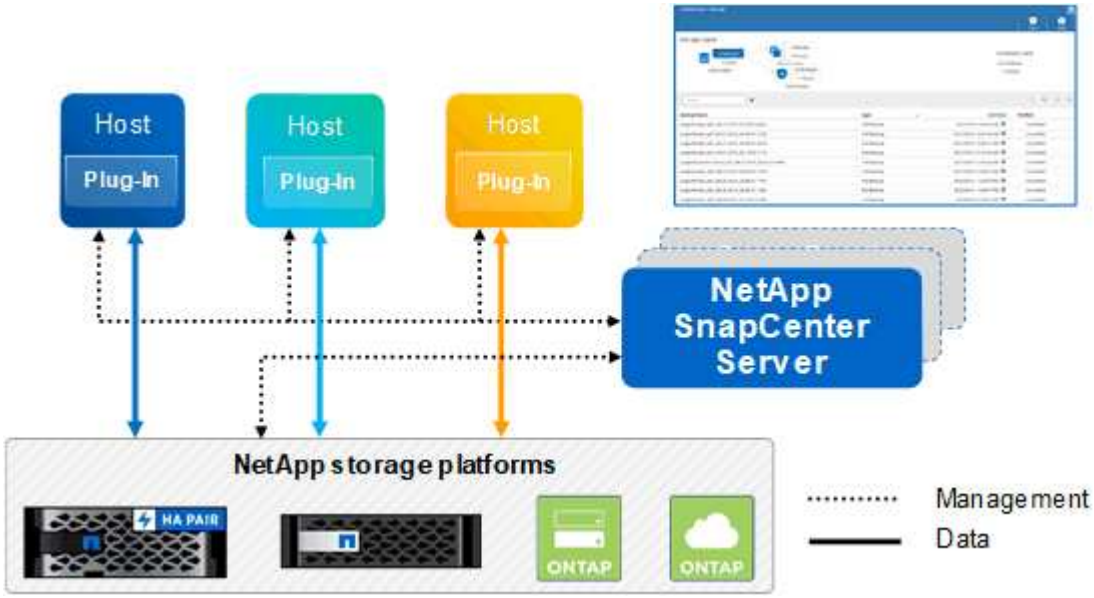
  Die Funktion für die synchrone Spiegelung ermöglicht eine Online-Datenreplizierung in Echtzeit zwischen Speicherarrays über Remote-Entfernungen.

  Weitere Informationen zur Sync-Spiegelung finden Sie unter "Übersicht über synchrones Spiegeln"

Architektur von SnapCenter

Die SnapCenter Plattform basiert auf einer mehrstufigen Architektur, die einen zentralen Management Server (SnapCenter Server) und einen SnapCenter Plug-in-Host umfasst.

SnapCenter unterstützt standortübergreifende Datacenter. Der SnapCenter-Server und der Plug-in-Host können sich an verschiedenen geografischen Standorten befinden.



Komponenten von SnapCenter

SnapCenter besteht aus SnapCenter Server und SnapCenter Plug-ins. Sie sollten nur die geeigneten Plug-ins für die Daten installieren, die Sie schützen möchten.

- SnapCenter Server
- Das SnapCenter Plug-ins-Paket für Windows enthält die folgenden Plug-ins:
  - SnapCenter Plug-in für Microsoft SQL Server
  - SnapCenter Plug-in für Microsoft Windows
  - SnapCenter Plug-in für Microsoft Exchange Server
  - SnapCenter-Plug-in für SAP HANA Database
  - SnapCenter Plug-in für IBM DB2
  - SnapCenter Plug-in für PostgreSQL
  - SnapCenter Plug-in für MySQL
  - SnapCenter Plug-in für MongoDB
  - SnapCenter Plug-in für ORASCPM (Oracle Applikationen)
  - SnapCenter Plug-in für SAP ASE
  - SnapCenter Plug-in für SAP MaxDB
  - SnapCenter Plug-in für Storage Plug-in
- Das SnapCenter Plug-ins-Paket für Linux umfasst die folgenden Plug-ins:
  - SnapCenter Plug-in für Oracle Database

    - SnapCenter-Plug-in für SAP HANA Database
    - SnapCenter Plug-in für UNIX Filesysteme
    - SnapCenter Plug-in für IBM DB2
    - SnapCenter Plug-in für PostgreSQL
    - SnapCenter Plug-in für MySQL
    - SnapCenter Plug-in für MongoDB
    - SnapCenter Plug-in für ORASCPM (Oracle Applikationen)
    - SnapCenter Plug-in für SAP ASE
    - SnapCenter Plug-in für SAP MaxDB
    - SnapCenter Plug-in für Storage Plug-in
- Das SnapCenter Plug-ins-Paket für AIX enthält die folgenden Plug-ins:
    - SnapCenter Plug-in für Oracle Database
    - SnapCenter Plug-in für UNIX Filesysteme
    - SnapCenter Plug-in für IBM DB2

Das SnapCenter Plug-in für VMware vSphere, vormals NetApp Data Broker, ist eine eigenständige virtuelle Appliance, die SnapCenter Datensicherungsvorgänge auf virtualisierten Datenbanken und Filesystemen unterstützt.

SnapCenter Server

Der SnapCenter Server umfasst einen Webserver, eine zentralisierte HTML5-basierte Benutzeroberfläche, PowerShell Commandlets, REST-APIs und das SnapCenter Repository.

SnapCenter Server unterstützt sowohl Microsoft Windows als auch Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5)

Wenn Sie das SnapCenter-Plug-ins-Paket für Linux oder das SnapCenter-Plug-ins-Paket für AIX verwenden, werden Zeitpläne zentral mit dem Quartz Scheduler ausgeführt.

- Für das SnapCenter-Plug-in für Oracle Database kommuniziert der Host-Agent, der auf dem SnapCenter Server-Host ausgeführt wird, mit dem SnapCenter-Plug-in-Loader (SPL), der auf dem Linux- oder AIX-Host ausgeführt wird, um verschiedene Datensicherungsvorgänge auszuführen.
- Beim SnapCenter-Plug-in für die SAP HANA-Datenbank kommuniziert der SnapCenter-Server mit dem Plug-in über den SCCore-Agenten, der auf dem Host ausgeführt wird.

Der SnapCenter-Server und die Plug-ins kommunizieren mit dem Host-Agent über HTTPS. Informationen zu den Vorgängen von SnapCenter werden im SnapCenter Repository gespeichert.

SnapCenter unterstützt ungemeinsamen Namespace für Windows Hosts. Wenn Sie Probleme bei der Verwendung von ungemeinsamen Namespace haben, lesen Sie "SnapCenter kann bei Verwendung von nicht gemeinsamem Namespace keine Ressourcen erkennen".

Sie sollten die folgenden Befehle ausführen, um den Status der SnapCenter-Komponenten zu erfahren, die auf dem Linux-Host ausgeführt werden:

- `systemctl status snapmanagerweb`
- `systemctl status scheduler`

- `systemctl status smcore`
- `systemctl status nginx`
- `systemctl status rabbitmq-server`

SnapCenter Plug-ins

Jedes SnapCenter-Plug-in unterstützt spezifische Umgebungen, Datenbanken und Applikationen.

Plug-in-Name	Im Installationspaket enthalten	Weitere Plug-ins sind erforderlich	Auf dem Host installiert	Unterstützte Plattformen
Plug-in für SQL Server	Plug-ins-Paket für Windows	Plug-in für Windows	SQL Server Host	Windows
Plug-in für Windows	Plug-ins-Paket für Windows		Windows Host	Windows
Plug-in für Exchange	Plug-ins-Paket für Windows	Plug-in für Windows	Exchange Server Host	Windows
Plug-in für Oracle Database	Plug-ins-Paket für Linux und Plug-ins-Paket für AIX	Plug-in für UNIX	Oracle Host	Linux oder AIX
Plug-in für SAP HANA Database	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	HDBSQL-Client-Host	Linux oder Windows
Plug-in für IBM DB2	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	DB2-Host	Linux oder Windows
Plug-in für PostgreSQL	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	PostgreSQL-Host	Linux oder Windows
Plug-in für MySQL	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Db2MySQL-Host	Linux oder Windows
Plug-in für MongoDB	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	MongoDB Host	Linux oder Windows
Plug-in für ORASCPM (Oracle Applikationen)	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Oracle Host	Linux oder Windows

Plug-in-Name	Im Installationspaket enthalten	Weitere Plug-ins sind erforderlich	Auf dem Host installiert	Unterstützte Plattformen
Plug-in für SAP ASE	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	SAP-Host	Linux oder Windows
Plug-in für SAP MaxDB	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	SAP MaxDB-Host	Linux oder Windows
Plug-in für Storage Plug-in	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Storage Host	Linux oder Windows

Das SnapCenter Plug-in für VMware vSphere unterstützt absturzkonsistente und VM-konsistente Backup- und Restore-Prozesse für Virtual Machines (VMs), Datastores und Virtual Machine Disks (VMDKs). Zudem unterstützt es die applikationsspezifischen Plug-ins von SnapCenter, um applikationskonsistente Backup- und Restore-Vorgänge für virtualisierte Datenbanken und Filesysteme zu sichern.

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für Benutzer, die SnapCenter 4.3 oder höher verwenden, enthält das "Dokumentation zum SnapCenter Plug-in für VMware vSphere" Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des Linux-basierten SnapCenter-Plug-ins für die virtuelle VMware vSphere-Appliance (Open Virtual Appliance Format).

SnapCenter Plug-in für Microsoft SQL Server Funktionen

- Automatisiert applikationsspezifische Backup-, Restore- und Klonvorgänge für Microsoft SQL Server Datenbanken in einer SnapCenter Umgebung.
- Unterstützt Microsoft SQL Server Datenbanken auf VMDK und RDM (Raw Device Mapping) LUNs bei der Bereitstellung des SnapCenter Plug-ins für VMware vSphere sowie bei der Registrierung des Plug-ins bei SnapCenter
- Unterstützt nur die Provisionierung von SMB-Freigaben. Für das Backup von SQL Server-Datenbanken auf SMB-Freigaben wird keine Unterstützung geboten.
- Unterstützt den Import von Backups von SnapManager für Microsoft SQL Server in SnapCenter.

SnapCenter Plug-in für Microsoft Windows Funktionen

- Ermöglicht die applikationsgerechte Datensicherung für andere Plug-ins, die auf Windows Hosts in Ihrer SnapCenter Umgebung laufen
- Automatisiert applikationsspezifische Backup-, Restore- und Klonvorgänge für Microsoft Filesysteme in Ihrer SnapCenter Umgebung

- Unterstützt Storage-Bereitstellung, Snapshot-Konsistenz und Speicherplatzrückgewinnung für Windows Hosts

> Das Plug-in für Windows stellt SMB-Freigaben und Windows-Filesysteme auf physischen und RDM-LUNs bereit, unterstützt jedoch keine Backup-Vorgänge für Windows File-Systeme auf SMB-Shares.

SnapCenter Plug-in für Microsoft Exchange Server Funktionen

- Automatisiert applikationsspezifische Backup- und Restore-Vorgänge für Microsoft Exchange Server Datenbanken und Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAGs) in Ihrer SnapCenter Umgebung
- Unterstützung virtualisierter Exchange Server auf RDM LUNs bei der Bereitstellung des SnapCenter Plug-in für VMware vSphere und Registrierung des Plug-ins bei SnapCenter

SnapCenter Plug-in für Oracle Database Funktionen

- Automatisierung applikationsspezifischer Backups, Restores, Recoverys, Überprüfung, Mounten, Unmounten und Klonen für Oracle Datenbanken in Ihrer SnapCenter Umgebung
- Unterstützung von Oracle-Datenbanken für SAP, aber die Integration von SAP BR*Tools ist nicht möglich

SnapCenter Plug-in für UNIX Funktionen

- Ermöglicht das Plug-in für Oracle Database die Durchführung von Datensicherungsvorgängen auf Oracle Datenbanken, indem es den zugrunde liegenden Host Storage Stack auf Linux oder AIX Systemen unterstützt
- Unterstützt NFS-Protokolle (Network File System) und SAN (Storage Area Network) auf einem Storage-System, auf dem ONTAP ausgeführt wird
- Bei Linux Systemen werden Oracle-Datenbanken auf VMDK und RDM-LUNs unterstützt, wenn Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.
- Unterstützt Mount Guard für AIX auf SAN-Dateisystemen und LVM-Layout.
- Unterstützt Enhanced Journaled File System (JFS2) mit Inline-Protokollierung auf SAN-Dateisystemen und LVM-Layout nur für AIX-Systeme.

  ES werden NATIVE SAN-Geräte, Dateisysteme und LVM-Layouts unterstützt, die auf SAN-Geräten basieren.

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

SnapCenter Plug-in für SAP HANA Database Funktionen

Automatisiert applikationsspezifische Backups, Restores und das Klonen von SAP HANA Datenbanken in der SnapCenter-Umgebung.

Von NetApp unterstützte Plug-ins-Funktionen

Von NetApp unterstützte Plug-ins sind MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und Storage Plug-in.

- Unterstützung anderer Plug-ins zum Management von Applikationen oder Datenbanken, die von anderen SnapCenter-Plug-ins nicht unterstützt werden Von NetApp unterstützte Plug-ins werden nicht als Teil der SnapCenter Installation bereitgestellt.
- Unterstützt die Erstellung von Spiegelkopien von Backup-Sätzen auf einem anderen Volume und die Disk-to-Disk Backup-Replizierung.
- Unterstützt sowohl Windows als auch Linux Umgebungen.

SnapCenter Plug-in für IBM DB2

Automatisiert applikationsspezifische Backups, Restores und das Klonen von IBM DB2 Datenbanken in der SnapCenter-Umgebung.

SnapCenter Plug-in für PostgreSQL

Automatisiert applikationsspezifische Backups, Restores und das Klonen von PostgreSQL Instanzen in der SnapCenter Umgebung.

SnapCenter Plug-in für MySQL

Automatisiert applikationsspezifische Backups, Restores und das Klonen von MySQL Instanzen in der SnapCenter Umgebung.

SnapCenter Repository

Das SnapCenter-Repository, auch als NSM-Datenbank bezeichnet, speichert Informationen und Metadaten für jede SnapCenter-Operation.

Die MySQL-Server-Repository-Datenbank wird standardmäßig bei der Installation des SnapCenter-Servers installiert. Wenn MySQL Server bereits installiert ist und Sie eine Neuinstallation von SnapCenter Server durchführen, sollten 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 verwendet haben, wird der MySQL Server während des SnapCenter-Upgrades auf 8.0.37 oder höher aktualisiert.

Das SnapCenter Repository speichert folgende Informationen und Metadaten:

- Metadaten für Backup, Klonen, Wiederherstellung und Verifizierung
- Reporting-, Job- und Ereignisinformationen
- Host- und Plug-in-Informationen
- Rollen-, Benutzer- und Berechtigungsdetails
- Informationen zur Storage-Systemverbindung

Sicherheitsfunktionen

SnapCenter setzt strenge Sicherheits- und Authentifizierungsfunktionen ein, damit Ihre Daten sicher bleiben.

SnapCenter umfasst die folgenden Sicherheitsfunktionen:

- Die gesamte Kommunikation zu SnapCenter verwendet HTTP über SSL (HTTPS).
- Alle Anmeldedaten in SnapCenter werden mit AES-Verschlüsselung (Advanced Encryption Standard) geschützt.
- SnapCenter verwendet Sicherheitsalgorithmen, die dem Federal Information Processing Standard (FIPS) entsprechen.
- SnapCenter unterstützt die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.
- SnapCenter 4.1.1 oder höher unterstützt TLS 1.2 (Transport Layer Security) für die Kommunikation mit ONTAP. Sie können TLS 1.2 auch für die Kommunikation zwischen Clients und Servern verwenden.

  Ab 5.0 unterstützt SnapCenter (TLS) 1.3 für die Kommunikation mit ONTAP.

- SnapCenter unterstützt einen bestimmten Satz von SSL-Cipher-Suites, um die Sicherheit der Netzwerkkommunikation zu gewährleisten.

  Weitere Informationen finden Sie unter "So konfigurieren Sie die unterstützte SSL Cipher Suite".

- SnapCenter wird innerhalb der Firewall Ihres Unternehmens installiert, um den Zugriff auf den SnapCenter Server zu ermöglichen und die Kommunikation zwischen dem SnapCenter Server und den Plug-ins zu ermöglichen.
- Für den SnapCenter-API- und -Betriebszugriff werden Tokens verwendet, die mit AES-Verschlüsselung verschlüsselt sind und nach 24 Stunden ablaufen.
- SnapCenter lässt sich zur Anmeldung und zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) in Windows Active Directory integrieren und ermöglicht die Zugriffsberechtigungen.
- IPsec wird mit SnapCenter unter ONTAP für Windows- und Linux-Hostcomputer unterstützt. "Weitere Informationen ."
- SnapCenter PowerShell Commandlets sind über die Sitzungen gesichert.
- Nach einer Standardlaufzeit von 15 Minuten Inaktivität warnt Sie SnapCenter, dass Sie in 5 Minuten abgemeldet werden. Nach 20 Minuten Inaktivität meldet SnapCenter Sie aus, und Sie müssen sich erneut anmelden. Sie können den Ausloggen Zeitraum ändern.
- Die Anmeldung ist nach 5 oder mehr falschen Anmeldeversuchen vorübergehend deaktiviert.
- Unterstützt CA-Zertifikatauthentifizierung zwischen SnapCenter-Server und ONTAP. "Weitere Informationen ."
- Integritätsprüfung wird dem SnapCenter-Server und den Plug-ins hinzugefügt und validiert alle im Lieferumfang enthaltenen Binärdateien bei Neuinstallationen und Upgrades.

ÜBERSICHT ÜBER DAS CA-Zertifikat

Das Installationsprogramm von SnapCenter Server ermöglicht die zentralisierte Unterstützung von SSL-Zertifikaten während der Installation. Um die sichere Kommunikation zwischen Server und Plug-in zu verbessern, unterstützt SnapCenter die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.

Sie sollten CA-Zertifikate bereitstellen, nachdem Sie den SnapCenter-Server und die entsprechenden Plug-ins installiert haben. Weitere Informationen finden Sie unter "ZertifikatCSR-Datei erstellen".

Sie können auch ein CA-Zertifikat für SnapCenter-Plug-in für VMware vSphere implementieren. Weitere Informationen finden Sie unter "Erstellen und Importieren von Zertifikaten".

Bidirektionale SSL-Kommunikation

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

Übersicht über die zertifikatbasierte Authentifizierung

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

Multi-Faktor-Authentifizierung (MFA)

MFA verwendet für das Management von Benutzersitzungen einen Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML) eines Drittanbieters. Diese Funktionalität verbessert die Authentifizierungssicherheit, da sie neben dem vorhandenen Benutzernamen und Passwort mehrere Faktoren wie TOTP, Biometrie, Push-Benachrichtigungen usw. verwenden kann. Zudem können Kunden mithilfe von IT-Providern ihre eigenen Benutzeridentitätsanbieter nutzen, um einheitliche SSO (Benutzeranmeldung) in ihrem gesamten Portfolio zu erhalten.

MFA ist nur für die Benutzerschnittstelle von SnapCenter Server anwendbar. Die Anmeldungen werden über die IdP Active Directory Federation Services (AD FS) authentifiziert. Sie können verschiedene Authentifizierungsfaktoren bei AD FS konfigurieren. SnapCenter ist der Service-Provider, und Sie sollten SnapCenter als eine abhängige Partei in AD FS konfigurieren. Um MFA in SnapCenter zu aktivieren, sind die AD FS-Metadaten erforderlich.

Informationen zum Aktivieren von MFA finden Sie unter "Multi-Faktor-Authentifizierung aktivieren".

Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter

RBAC-Typen

Mit der rollenbasierten Zugriffssteuerung (RBAC) und den ONTAP Berechtigungen von SnapCenter können SnapCenter Administratoren die Kontrolle über SnapCenter Ressourcen an verschiedene Benutzer oder Benutzergruppen delegieren. Dank dieses zentral gemanagten Zugriffs können Applikationsadministratoren innerhalb delegierter Umgebungen sicher arbeiten.

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

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

SnapCenter verwendet folgende Arten der rollenbasierten Zugriffssteuerung:

- RBAC von SnapCenter

- SnapCenter Plug-in RBAC (für einige Plug-ins)
- RBAC auf Applikationsebene
- ONTAP-Berechtigungen

RBAC von SnapCenter

Rollen und Berechtigungen

SnapCenter wird mit vordefinierten Rollen ausgeliefert, deren Berechtigungen bereits zugewiesen sind. Sie können diesen Rollen Benutzer oder Benutzergruppen zuweisen. Sie können auch neue Rollen erstellen und Berechtigungen und Benutzer verwalten.

Zuweisen von Berechtigungen für Benutzer oder Gruppen

Sie können Benutzern oder Gruppen Berechtigungen zuweisen, um auf SnapCenter-Objekte wie Hosts, Speicherverbindungen und Ressourcengruppen zuzugreifen. Sie können die Berechtigungen der SnapCenterAdmin-Rolle nicht ändern.

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

> Wenn Sie eine benutzerdefinierte Rolle erstellen, muss sie alle Berechtigungen der SnapCenter-Administratorrolle enthalten. Wenn Sie nur einige der Berechtigungen kopieren, z. B. Host add oder Host remove, können Sie diese Vorgänge nicht ausführen.

Authentifizierung

Benutzer müssen bei der Anmeldung über die grafische Benutzeroberfläche (GUI) oder PowerShell Commandlets über die Authentifizierung sorgen. Wenn Benutzer Mitglieder mehrerer Rollen sind, werden sie nach der Eingabe von Anmeldedaten aufgefordert, die gewünschte Rolle anzugeben. Benutzer müssen außerdem eine Authentifizierung zur Ausführung der APIs bereitstellen.

RBAC auf Applikationsebene

SnapCenter verwendet die Zugangsdaten, um sicherzustellen, dass autorisierte SnapCenter Benutzer auch über Berechtigungen auf Applikationsebene verfügen.

Wenn Sie beispielsweise Snapshot- und Datensicherungsvorgänge in einer SQL Server-Umgebung durchführen möchten, müssen Sie Anmeldedaten mit den richtigen Windows- oder SQL-Anmeldedaten festlegen. Der SnapCenter-Server authentifiziert die Anmeldeinformationen, die auf beiden Methoden festgelegt sind. Wenn Sie Snapshot- und Datensicherungsvorgänge in einer Windows-Dateisystemumgebung auf ONTAP-Speicher ausführen möchten, muss die SnapCenter-Administratorrolle über Administratorrechte auf dem Windows-Host verfügen.

Wenn Sie Datensicherungsvorgänge in einer Oracle-Datenbank durchführen möchten und wenn die Betriebssystemauthentifizierung im Datenbank-Host deaktiviert ist, müssen Sie die Anmeldedaten mit der Oracle-Datenbank oder den Oracle-ASM-Anmeldeinformationen festlegen. Der SnapCenter-Server authentifiziert die Anmeldeinformationen, die mit einer dieser Methoden festgelegt wurden, je nach Operation.

SnapCenter Plug-in für VMware vSphere RBAC

Wenn Sie das SnapCenter VMware Plug-in für die VM-konsistente Datensicherung nutzen, bietet der vCenter

Server zusätzliche RBAC-Level. Das SnapCenter VMware Plug-in unterstützt sowohl vCenter Server RBAC als auch Data ONTAP RBAC.

Weitere Informationen finden Sie unter "SnapCenter Plug-in für VMware vSphere RBAC"

ONTAP-Berechtigungen

Sie sollten vsadmin-Konto mit den erforderlichen Berechtigungen für den Zugriff auf das Speichersystem erstellen.

Informationen zum Erstellen des Kontos und Zuweisen von Berechtigungen finden Sie unter "Erstellen einer ONTAP-Cluster-Rolle mit minimalen Berechtigungen"

RBAC-Berechtigungen und -Rollen

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter können Sie Rollen erstellen und diesen Rollen Berechtigungen zuweisen und dann den Rollen Benutzer oder Benutzergruppen zuweisen. So können SnapCenter Administratoren eine zentral verwaltete Umgebung erstellen, während Applikationsadministratoren die Datensicherung managen können. SnapCenter wird mit vordefinierten Rollen und Berechtigungen ausgeliefert.

SnapCenter Rollen

SnapCenter wird mit den folgenden vordefinierten Rollen ausgeliefert. Sie können diesen Rollen Benutzer und Gruppen zuweisen oder neue Rollen erstellen.

Wenn Sie einem Benutzer eine Rolle zuweisen, werden auf der Seite „Jobs“ nur Aufträge angezeigt, die für diesen Benutzer relevant sind, es sei denn, Sie haben die Rolle „SnapCenter-Admin“ zugewiesen.

- Administrator für App Backup und Klonen
- Backup und Clone Viewer
- Infrastrukturadministrator
- SnapCenterAdmin

SnapCenter Plug-in für VMware vSphere Rollen

Für das Management der VM-konsistenten Datensicherung von VMs, VMDKs und Datastores werden in vCenter die folgenden Rollen vom SnapCenter Plug-in für VMware vSphere erstellt:

- SCV Administrator
- SCV-Ansicht
- SCV-Backup
- SCV-Wiederherstellung
- Wiederherstellung der SCV-Gastdatei

Weitere Informationen finden Sie unter "RBAC-Typen für SnapCenter Plug-in für VMware vSphere Benutzer"

Best Practice: NetApp empfiehlt, eine ONTAP-Rolle für das SnapCenter Plug-in für VMware vSphere Operationen zu erstellen und diese alle erforderlichen Berechtigungen zuzuweisen.

SnapCenter-Berechtigungen

SnapCenter bietet folgende Berechtigungen:

- Ressourcengruppe
- Richtlinie
- Backup
- Host
- Storage-Anbindung
- Klonen
- Bereitstellung (nur für Microsoft SQL Datenbank)
- Dashboard
- Berichte An
- Wiederherstellen
- Ressource

  Für nicht-Administratoren sind vom Administrator Plug-in-Berechtigungen erforderlich, um eine Ressourcenerkennung durchzuführen.

- Plug-in Installieren oder Deinstallieren

  Wenn Sie die Berechtigungen für die Plug-in-Installation aktivieren, müssen Sie auch die Host-Berechtigung ändern, um Lese- und Updates zu aktivieren.

- Migration
- Mount (nur für Oracle Database)
- Unmount (nur für Oracle Database)
- Job-Überwachung

  Mit der Berechtigung Job Monitor können Mitglieder verschiedener Rollen die Vorgänge für alle Objekte anzeigen, denen sie zugewiesen sind.

Vordefinierte SnapCenter-Rollen und -Berechtigungen

Im Lieferumfang von SnapCenter sind vordefinierte Rollen enthalten, von denen jede bereits aktiviert ist. Beim Einrichten und Verwalten der rollenbasierten Zugriffssteuerung können Sie entweder die vordefinierten Rollen verwenden oder neue erstellen.

SnapCenter umfasst die folgenden vordefinierten Rollen:

- SnapCenter Administratorrolle
- Administratorrolle für App Backup und Klonen

- Backup und Clone Viewer-Rolle
- Rolle für den Infrastrukturadministrator

Wenn Sie einem Benutzer einer Rolle hinzufügen, müssen Sie entweder die Berechtigung StorageConnection zuweisen, um die Kommunikation mit der Storage Virtual Machine (SVM) zu aktivieren, oder dem Benutzer eine SVM zuweisen, damit die Berechtigung zur Verwendung der SVM aktiviert wird. Mit der Berechtigung für Speicherverbindungen können Benutzer SVM-Verbindungen erstellen.

Ein Benutzer mit der Rolle „SnapCenter-Admin“ kann beispielsweise SVM-Verbindungen erstellen und einem Benutzer mit der Rolle „App-Backup“ und „Clone Admin“ zuweisen. Dieser besitzt standardmäßig keine Berechtigung, SVM-Verbindungen zu erstellen oder zu bearbeiten. Ohne SVM-Verbindung können Benutzer Backup-, Klon- oder Restore-Vorgänge nicht abschließen.

SnapCenter Administratorrolle

In der 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.

Administratorrolle für App Backup und Klonen

Die Rolle „App Backup“ und „Clone Admin“ verfügt über die erforderlichen Berechtigungen zur Durchführung administrativer Aktionen für Applikations-Backups und klonbezogene Aufgaben. Diese Rolle verfügt nicht über Berechtigungen für Host-Management, Bereitstellung, Storage-Verbindungs-Management oder Remote-Installation.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
Ressourcengruppe	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Richtlinie	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Backup	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Host	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Storage-Anbindung	Keine Angabe	Nein	Ja.	Nein	Nein
Klonen	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Bereitstellung	Keine Angabe	Nein	Ja.	Nein	Nein
Dashboard	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Berichte An	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Wiederherstellen	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
Ressource	Ja.	Ja.	Ja.	Ja.	Ja.
Plug-in Installation/Deinstallation	Nein	Keine Angabe		Keine Angabe	Keine Angabe
Migration	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Montieren	Ja.	Ja.	Keine Angabe	Keine Angabe	Keine Angabe
Unmounten	Ja.	Ja.	Keine Angabe	Keine Angabe	Keine Angabe
Vollständige Volume-Wiederherstellung	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Backup und Clone Viewer-Rolle

Die Rolle Backup und Clone Viewer verfügt über eine schreibgeschützte Ansicht aller Berechtigungen. In dieser Rolle sind auch Berechtigungen für Erkennung, Berichterstellung und Zugriff auf das Dashboard aktiviert.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
Ressourcengruppe	Keine Angabe	Nein	Ja.	Nein	Nein
Richtlinie	Keine Angabe	Nein	Ja.	Nein	Nein
Backup	Keine Angabe	Nein	Ja.	Nein	Nein
Host	Keine Angabe	Nein	Ja.	Nein	Nein
Storage-Anbindung	Keine Angabe	Nein	Ja.	Nein	Nein
Klonen	Keine Angabe	Nein	Ja.	Nein	Nein
Bereitstellung	Keine Angabe	Nein	Ja.	Nein	Nein
Dashboard	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
Berichte An	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Wiederherstellen	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Ressource	Nein	Nein	Ja.	Ja.	Nein
Plug-in Installation/Deinstallation	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Migration	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Montieren	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Unmounten	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Vollständige Volume-Wiederherstellung	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Rolle für den Infrastrukturadministrator

Die Rolle „Infrastrukturadministrator“ hat Berechtigungen für Host-Management, Storage-Management, Bereitstellung, Ressourcengruppen, Remote-Installationsberichte, Zugriff auf das Dashboard.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
Ressourcengruppe	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Richtlinie	Keine Angabe	Nein	Ja.	Ja.	Ja.
Backup	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Host	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Storage-Anbindung	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Klonen	Keine Angabe	Nein	Ja.	Nein	Nein

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
Bereitstellung	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Dashboard	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Berichte An	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Wiederherstellen	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Ressource	Ja.	Ja.	Ja.	Ja.	Ja.
Plug-in Installation/Deinstallation	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Migration	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Montieren	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Unmounten	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Vollständige Volume-Wiederherstellung	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

SnapCenter Disaster Recovery

Mithilfe der Disaster Recovery-Funktion von SnapCenter können Sie den SnapCenter Server im Falle von Ausfällen wie einer Beschädigung von Ressourcen oder einem Serverabsturz wiederherstellen. Sie können SnapCenter Repositorys, Serverzeitpläne und Serverkonfigurationskomponenten wiederherstellen. Sie können auch das SnapCenter Plug-in für SQL Server und das SnapCenter Plug-in für SQL Server Storage wiederherstellen.

In diesem Abschnitt werden die beiden Arten der Disaster Recovery (DR) in SnapCenter beschrieben:

DR mit SnapCenter Servern

- Die Daten des SnapCenter Servers werden gesichert und können ohne Plug-in wiederhergestellt werden, das dem SnapCenter Server hinzugefügt oder durch ihn gemanagt wird.
- Der sekundäre SnapCenter Server sollte auf demselben Installationsverzeichnis und auf demselben Port wie der primäre SnapCenter-Server installiert sein.

- Für die Multi-Faktor-Authentifizierung (MFA) schließen Sie während der SnapCenter-Server-Wiederherstellung alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um sich erneut anzumelden. Dadurch werden die vorhandenen oder aktiven Sitzungscookies gelöscht und die korrekten Konfigurationsdaten aktualisiert.
- Die Disaster Recovery-Funktion von SnapCenter verwendet FÜR das Backup des SnapCenter Servers REST-APIs. Siehe "REST-API-Workflows für Disaster Recovery von SnapCenter Server".
- Die Konfigurationsdatei für die Audit-Einstellungen wird nicht im DR-Backup gesichert und auch nicht auf dem DR-Server nach dem Wiederherstellungsvorgang. Sie sollten die Einstellungen für das Überwachungsprotokoll manuell wiederholen.

SnapCenter Plug-in und Storage DR

DR wird nur für das SnapCenter Plug-in für SQL Server unterstützt. Wenn das SnapCenter-Plug-in für SQL Server ausfällt, wechseln Sie zu einem anderen SQL-Host und stellen Sie die Daten mit wenigen Schritten wieder her. Siehe "Disaster Recovery eines SnapCenter Plug-ins für SQL Server".

SnapCenter nutzt ONTAP SnapMirror Technologie zur Datenreplizierung. Er kann zur DR an einem sekundären Standort repliziert und synchron gehalten werden. Ein Failover kann durch die Unterbrechung der Replizierungsbeziehung in SnapMirror initiiert werden. Während Failback kann die Synchronisierung umgekehrt werden und Daten vom DR-Standort zurück zum primären Standort repliziert werden.

Ressourcen, Ressourcengruppen und Richtlinien

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- **Ressourcen** sind normalerweise Datenbanken, Windows-Dateisysteme oder File Shares, die Sie mit SnapCenter sichern oder klonen.

  Je nach Umgebung können es sich jedoch um Ressourcen wie Datenbankinstanzen, Microsoft SQL Server Availability Groups, Oracle Datenbanken, Oracle RAC Datenbanken, Windows File-Systeme oder eine Gruppe benutzerdefinierter Applikationen handeln.

- Eine **Ressourcengruppe** ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Die Ressourcengruppe kann auch Ressourcen von mehreren Hosts und mehreren Clustern enthalten.

  Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für alle Ressourcen aus, die in der Ressourcengruppe gemäß dem von Ihnen für die Ressourcengruppe festgelegten Zeitplan definiert sind.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen konfigurieren.

  > ⓘ Wenn Sie einen Host einer Gruppe gemeinsam genutzter Ressourcen in den Wartungsmodus versetzen und Pläne mit derselben gemeinsam genutzten Ressourcengruppe verknüpft sind, werden alle geplanten Vorgänge für alle anderen Hosts der gemeinsam genutzten Ressourcengruppe ausgesetzt.

  Sie sollten ein Datenbank-Plug-in zum Sichern von Datenbanken, ein Filesystem-Plug-in zum Backup von Filesystemen und das SnapCenter Plug-in für VMware vSphere zum Sichern von VMs und Datastores verwenden.

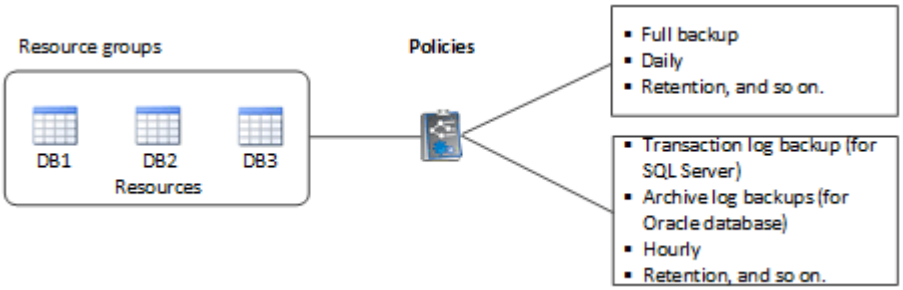
- **Richtlinien** Geben Sie die Backup-Häufigkeit, die Aufbewahrung von Kopien, die Replikation, Skripte und andere Merkmale von Datenschutzvorgängen an.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf ausführen.

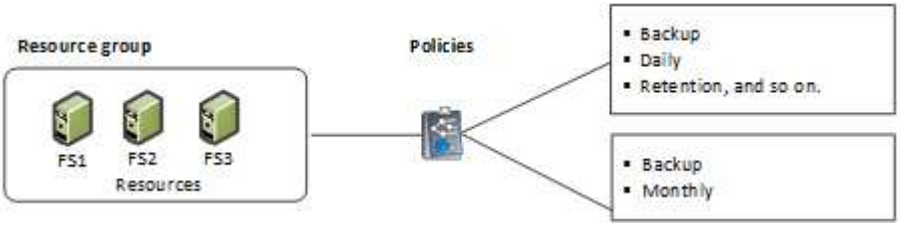
Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme des Hosts enthält. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik.

Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass sie täglich ein vollständiges Backup durchführt, und einen anderen Zeitplan, der stündlich Protokoll-Backups durchführt.

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



Die folgende Abbildung veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Windows File-Systeme:



Vorschriften und Postskripte

Im Rahmen Ihrer Datensicherungsabläufe können Sie benutzerdefinierte Prescripts und Postskripte verwenden. Diese Skripte ermöglichen die Automatisierung entweder vor oder nach Ihrem Datensicherungsauftrag. Sie können z. B. ein Skript einschließen, das Sie automatisch über Fehler oder Warnungen bei Datenschutzaufstellungsfehlern benachrichtigt. Bevor Sie Ihre Prescripts und Postscripts einrichten, sollten Sie einige der Anforderungen zur Erstellung dieser Skripte kennen.

Unterstützte Skripttypen

Die folgenden Skripttypen werden für Windows unterstützt:

- Batch-Dateien
- PowerShell Skripte
- Perl-Skripte

Für UNIX werden die folgenden Skripttypen unterstützt:

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

> Zusammen mit Standard-Bash-Shell werden auch andere Shells wie sh-Shell, k-shell und c-shell unterstützt.

Skriptpfad

Alle im Rahmen des SnapCenter Betriebs ausgeführten Prescripts und Postskripte auf nicht virtualisierten und virtualisierten Storage-Systemen werden auf dem Plug-in Host ausgeführt.

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

> Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares 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.

Angeben von Skripten

Skripte werden in den Backup-Richtlinien angegeben. Wenn ein Sicherungsauftrag gestartet wird, ordnet die Richtlinie das Skript automatisch den gesicherten Ressourcen zu. Wenn Sie eine Sicherungsrichtlinie erstellen, können Sie die Vorschrift- und die Postscript-Argumente angeben.

> Sie können nicht mehrere Skripte angeben.

Skript-Timeouts

Die Zeitüberschreitung ist standardmäßig auf 60 Sekunden eingestellt. Sie können den Zeitüberschreitungswert ändern.

Skriptausgabe

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

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

SnapCenter-Automatisierung mit REST-APIs

MITHILFE VON REST-APIs lassen sich verschiedene SnapCenter-Managementvorgänge ausführen. REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um die REST-API-Dokumentation anzuzeigen und einen API-Aufruf manuell zu tätigen. Mit REST-APIs können Sie Ihren SnapCenter Server oder Ihren SnapCenter vSphere Host managen.

DIE REST-APIs für…	Befinden sich in…
SnapCenter Server	\Https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/
SnapCenter Plug-in für VMware vSphere	\Https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/API/swagger-ui.HTML#

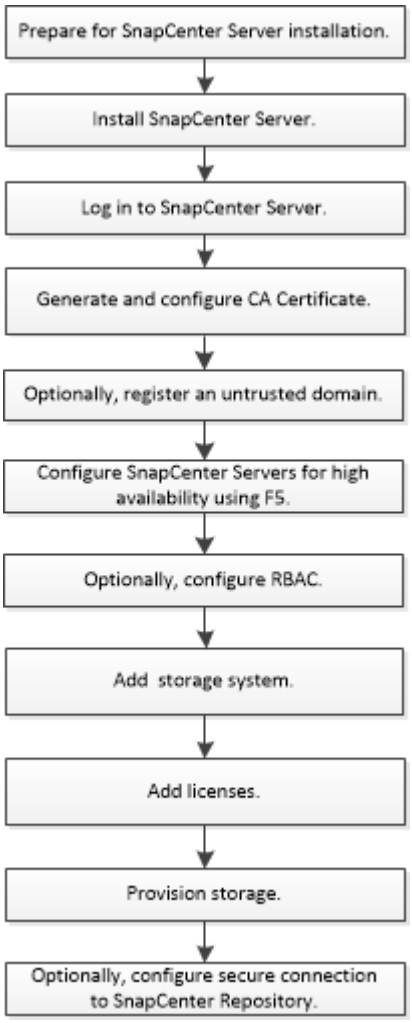
Weitere Informationen zu SnapCenter REST-APIs finden Sie unter "Übersicht ÜBER REST-APIs"

Weitere Informationen zum SnapCenter-Plug-in für VMware vSphere REST-APIs finden Sie unter "SnapCenter Plug-in für VMware vSphere REST-APIs"

Installation von SnapCenter Server

Installations-Workflow

Der Workflow zeigt die verschiedenen Aufgaben, die für die Installation und Konfiguration des SnapCenter-Servers erforderlich sind.



Bereiten Sie sich auf die Installation des SnapCenter-Servers vor

Anforderungen an Domäne und Arbeitsgruppe

Der SnapCenter-Server kann auf Systemen installiert werden, die sich entweder in einer Domäne oder in einer Arbeitsgruppe befinden. Der für die Installation verwendete Benutzer muss bei Arbeitsgruppen und Domänen über Administratorrechte auf dem Computer verfügen.

Für die Installation von SnapCenter Server und SnapCenter Plug-ins auf Windows Hosts sollten Sie einen der folgenden Schritte verwenden:

- **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.

Obwohl Domänen-Trusts, Multi-Domain-Wälder und domänenübergreifende Trusts unterstützt werden, werden forstübergreifende Domänen nicht unterstützt. Die Microsoft-Dokumentation zu Active Directory-Domänen und Trusts enthält weitere Informationen.

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

Platz- und Größenanforderungen

Vor der Installation des SnapCenter Servers sollten Sie mit den Platz- und Größenanforderungen vertraut sein. Sie sollten auch die verfügbaren System- und Sicherheitsupdates anwenden.

Element	Windows-Host-Anforderungen	Anforderungen an Linux-Hosts
Betriebssysteme	Microsoft Windows Es werden nur englische, deutsche, japanische und vereinfachte chinesische Versionen der Betriebssysteme unterstützt. Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".	• Red hat Enterprise Linux (RHEL) 8 und 9 • SUSE Linux Enterprise Server (SLES) 15 Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".
Minimale CPU-Anzahl	4 Kerne	4 Kerne
Mind. RAM	8GB Der MySQL Server Pufferpool nutzt 20 Prozent des gesamten RAM.	8GB

Element	Windows-Host-Anforderungen	Anforderungen an Linux-Hosts
Minimaler Festplattenspeicher für die SnapCenter-Serversoftware und Protokolle	7GB Wenn sich das SnapCenter-Repository auf demselben Laufwerk befindet, auf dem SnapCenter-Server installiert ist, wird empfohlen, 15 GB zu verwenden.	15GB
Minimaler Festplattenspeicher für das SnapCenter-Repository	8GB HINWEIS: Wenn der SnapCenter-Server auf demselben Laufwerk installiert ist, auf dem das SnapCenter-Repository installiert ist, wird empfohlen, 15 GB zu verwenden.	Keine Angabe
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 oder höher • ASP.NET Core Hosting Bundle ab Version 8.0.5 mit allen nachfolgenden .NET 8 Patches • PowerShell 7.4.2 oder höher Für . NETZSPEZIFISCHE Informationen zur Fehlerbehebung, siehe "SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl".	• ASP.NET Core Runtime beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell 7.4.2 oder höher • Nginx ist ein Webserver, der als Reverse Proxy verwendet werden kann • PAM-Entwicklung PAM (Pluggable Authentication Modules) ist ein Systemsicherheitstool, mit dem Systemadministratoren Authentifizierungsrichtlinien festlegen können, ohne Programme neu kompilieren zu müssen, die die Authentifizierung durchführen.

SAN-Host-Anforderungen

Wenn Ihr SnapCenter Host Teil einer FC-/iSCSI-Umgebung ist, müssen Sie möglicherweise zusätzliche Software auf dem System installieren, um den Zugriff auf ONTAP Storage zu ermöglichen.

SnapCenter umfasst keine Host Utilities oder DSM. Wenn Ihr SnapCenter Host Teil einer SAN-Umgebung ist, müssen Sie eventuell die folgende Software installieren und konfigurieren:

- Host Utilities

  Die Host Utilities unterstützen FC und iSCSI, und es ermöglicht Ihnen die Verwendung von MPIO auf Ihren Windows Servern. Weitere Informationen finden Sie unter "Host Utilities-Dokumentation".

- Microsoft DSM für Windows MPIO

  Diese Software arbeitet mit Windows MPIO-Treibern für das Management mehrerer Pfade zwischen NetApp und Windows Host-Computern zusammen.

  DSM ist für Hochverfügbarkeitskonfigurationen erforderlich.

  Wenn Sie ONTAP DSM verwenden, sollten Sie zu Microsoft DSM migrieren. Weitere Informationen finden Sie unter "So migrieren Sie von ONTAP DSM zu Microsoft DSM".

Unterstützte Storage-Systeme und Applikationen

Sie sollten die unterstützten Storage-Systeme, Applikationen und Datenbanken kennen.

- SnapCenter unterstützt ONTAP 9.12.1 und neuere Versionen für den Schutz Ihrer Daten.
- SnapCenter unterstützt Amazon FSX für NetApp ONTAP, um Ihre Daten vor der SnapCenter Software 4.5 P1-Patch-Veröffentlichung zu schützen.

  Wenn Sie Amazon FSX für NetApp ONTAP verwenden, stellen Sie sicher, dass die SnapCenter Server Host-Plug-ins auf 4.5 P1 oder höher aktualisiert werden, um Datensicherungsprozesse zu auszuführen.

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

  Weitere Informationen zu Amazon FSX for NetApp ONTAP finden Sie unter "Dokumentation zu Amazon FSX für NetApp ONTAP".

- SnapCenter unterstützt den Schutz verschiedener Applikationen und Datenbanken.

  Ausführliche Informationen zu den unterstützten Anwendungen und Datenbanken finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

- SnapCenter 4.9 P1 und höher unterstützt den Schutz von Oracle- und Microsoft-SQL-Workloads in VMware Cloud auf AWS-Umgebungen (Software-Defined Data Center) von Amazon Web Services.

  Weitere Informationen finden Sie unter "Schützen Sie Oracle- und MS-SQL-Workloads mithilfe von NetApp SnapCenter in VMware Cloud auf AWS SDDC-Umgebungen".

Unterstützte Browser

SnapCenter-Software kann auf mehreren Browsern verwendet werden.

- Chrome-Version 125 und höher
- Microsoft Edge 110.0.1587.17 und höher

Aktuelle Informationen zu unterstützten Versionen finden Sie unter : "NetApp Interoperabilitäts-Matrix-Tool".

Verbindungs- und Portanforderungen

Stellen Sie sicher, dass die Verbindungs- und Ports-Anforderungen erfüllt sind, bevor Sie die SnapCenter Server- und Applikations- oder Datenbank-Plug-ins installieren.

- Anwendungen können einen Port nicht gemeinsam nutzen.

  Jeder Port muss der entsprechenden Applikation zugeordnet sein.

- Bei anpassbaren Ports können Sie während der Installation einen benutzerdefinierten Port auswählen, wenn Sie den Standardport nicht verwenden möchten.

  Sie können einen Plug-in-Port nach der Installation mithilfe des Assistenten zum Ändern von Hosts ändern.

- Für feste Ports sollten Sie die Standard-Port-Nummer akzeptieren.
- Firewalls
  - Firewalls, Proxys oder andere Netzwerkgeräte sollten keine Verbindung stören.
  - Wenn Sie bei der Installation von SnapCenter einen benutzerdefinierten Port angeben, sollten Sie auf dem Plug-in-Host eine Firewall-Regel für diesen Port für den SnapCenter-Plug-in-Loader hinzufügen.

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

Typ des Ports	Standardport
SnapCenter-Port	8146 (HTTPS), bidirektional, anpassbar, wie in der URL *https://server:8146* Wird für die Kommunikation zwischen dem SnapCenter-Client (dem SnapCenter-Benutzer) und dem SnapCenter-Server verwendet. Wird auch zur Kommunikation von den Plug-in-Hosts mit dem SnapCenter-Server verwendet. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."

Typ des Ports	Standardport
SnapCenter SMCore-Kommunikations-Port	8145 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen dem SnapCenter-Server und den Hosts verwendet, auf denen die SnapCenter-Plug-ins installiert sind. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."
Scheduler-Service-Port	8154 (HTTPS) Über diesen Port werden die SnapCenter-Scheduler-Workflows für alle gemanagten Plug-ins im SnapCenter Server Host zentral orchestriert. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."
RabbitMQ-Anschluss	5672 (tcp) Dies ist der Standardport, den RabbitMQ abhört und der für die Kommunikation zwischen dem Scheduler-Dienst und dem SnapCenter zwischen dem Publisher-Subscriber-Modell verwendet wird.
MySQL-Anschluss	3306 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen SnapCenter und der MySQL Repository Datenbank verwendet. Sie können sichere Verbindungen vom SnapCenter-Server zum MySQL-Server erstellen. "Weitere Informationen ." Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."

Typ des Ports	Standardport
Windows Plug-in-Hosts	135, 445 (TCP) Neben den Ports 135 und 445 sollte auch der von Microsoft festgelegte dynamische Portbereich geöffnet sein. Remote-Installationsvorgänge verwenden den Windows Management Instrumentation (WMI)-Dienst, der diesen Portbereich dynamisch durchsucht. Informationen zum unterstützten dynamischen Portbereich finden Sie unter "Serviceübersicht und Netzwerkanschlussanforderungen für Windows" Die Ports dienen zur Kommunikation zwischen dem SnapCenter-Server und dem Host, auf dem das Plug-in installiert wird. Um Plug-in-Binärdateien auf Windows-Plug-in-Hosts zu übertragen, müssen die Ports nur auf dem Plug-in-Host geöffnet sein, und sie können nach der Installation geschlossen werden.
Linux- oder AIX-Plug-in-Hosts	22 (SSH) Die Ports dienen zur Kommunikation zwischen dem SnapCenter-Server und dem Host, auf dem das Plug-in installiert wird. Die Ports werden von SnapCenter verwendet, um Plug-in-Paketbinärdateien auf Linux- oder AIX-Plug-in-Hosts zu kopieren. Sie sollten von der Firewall oder von iptables geöffnet oder ausgeschlossen sein.
SnapCenter-Plug-ins-Paket für Windows, SnapCenter-Plug-ins-Paket für Linux oder SnapCenter-Plug-ins-Paket für AIX	8145 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen SMCore und Hosts verwendet, auf denen das Plug-ins-Paket installiert ist. Der Kommunikationspfad muss auch zwischen der SVM-Management-LIF und dem SnapCenter-Server offen sein. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows" oder "Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."

Typ des Ports	Standardport
SnapCenter Plug-in für Oracle Database	27216, anpassbar Der Standard-JDBC-Port wird vom Plug-in für Oracle für die Verbindung mit der Oracle-Datenbank verwendet. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."
SnapCenter Plug-in für Exchange Datenbank	909, anpassbar Das Standard-NET. Der TCP-Port wird vom Plug-in für Windows für die Verbindung mit Exchange VSS-Rückrufen verwendet. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie das Plug-in für Exchange".
Von NetApp unterstützte Plug-ins für SnapCenter	9090 (HTTPS), fest Dies ist ein interner Port, der nur auf dem von NetApp unterstützten Plug-In-Host verwendet wird. Es ist keine Firewall-Ausnahme erforderlich. Die Kommunikation zwischen dem SnapCenter-Server und den von NetApp unterstützten Plug-Ins wird über Port 8145 geleitet.
ONTAP-Cluster oder SVM-Kommunikations-Port	443 (HTTPS), bidirectional80 (HTTP), bidirektional Der Port wird von der SAL (Storage Abstraction Layer) für die Kommunikation zwischen dem Host verwendet, auf dem SnapCenter-Server und SVM ausgeführt wird. Der Port wird zur Kommunikation zwischen dem SnapCenter Plug-in-Host und der SVM derzeit auch von der SAL on SnapCenter für Windows Plug-in-Hosts verwendet.

Typ des Ports	Standardport
SnapCenter-Plug-in für SAP HANA-Datenbank vCode Zauber-Checkerports	3instance_number13 or 3instance_number15, HTTP oder HTTPS, bidirektional und anpassbar Bei einem einzelnen Mandanten mit mandantenfähigen Datenbank-Containern (MDC) endet die Port-Nummer mit 13. Für einen nicht-MDC-Server endet die Port-Nummer mit 15. Beispielsweise ist 32013 die Portnummer für die Instanz 20 und 31015 die Portnummer für Instanz 10. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts."
Kommunikations-Port des Domänencontrollers	In der Microsoft-Dokumentation finden Sie Informationen zu den Ports, die in der Firewall auf einem Domänencontroller geöffnet werden sollen, damit die Authentifizierung ordnungsgemäß funktioniert. Es ist erforderlich, die erforderlichen Microsoft-Ports auf dem Domänen-Controller zu öffnen, damit der SnapCenter-Server, Plug-in-Hosts oder andere Windows-Client die Benutzer authentifizieren kann.

Informationen zum Ändern der Portdetails finden Sie unter "Ändern Sie die Plug-in-Hosts".

SnapCenter-Lizenzen

Für die Datensicherung von Applikationen, Datenbanken, Filesystemen und Virtual Machines benötigt SnapCenter mehrere Lizenzen. Die Art der installierten SnapCenter Lizenzen hängt von Ihrer Storage-Umgebung und den gewünschten Funktionen ab.

Lizenz	Bei Bedarf
SnapCenter Standard Controller-basiert	Erforderlich für FAS, AFF, All-SAN-Array (ASA) Bei der SnapCenter Standardlizenz handelt es sich um eine Controller-basierte Lizenz, die als Teil von ONTAP One enthalten ist. Wenn Sie die Lizenz für die SnapManager Suite besitzen, erhalten Sie auch die Standardlizenz von SnapCenter. Wenn Sie SnapCenter als Testlizenz mit FAS, AFF oder ASA Storage installieren möchten, erhalten Sie bei Ihrem Vertriebsmitarbeiter eine Evaluierungslizenz für ONTAP One. Informationen zu Lizenzen, die in ONTAP One enthalten sind, finden Sie unter "In ONTAP One enthaltene Lizenzen". SnapCenter ist auch als Teil des Datensicherungs-Bundles verfügbar. Wenn Sie A400 oder höher erworben haben, sollten Sie ein Datensicherungs-Bundle erwerben.
SnapMirror oder SnapVault	ONTAP Wenn die Replizierung in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault Lizenz erforderlich.
SnapRestore	Für die Wiederherstellung und Überprüfung von Backups erforderlich. Auf primären Storage-Systemen • Erforderlich auf SnapVault Zielsystemen, um eine Remote-Verifizierung und die Wiederherstellung aus einem Backup durchzuführen. • Erforderlich auf SnapMirror Zielsystemen für die Remote-Verifizierung

Lizenz	Bei Bedarf
FlexClone	Die für das Klonen von Datenbanken und Verifizierungsvorgängen erforderlich sind. Auf primären und sekundären Storage-Systemen • Erforderlich auf SnapVault Zielsystemen, um Klone aus dem sekundären Vault Backup zu erstellen. • Erforderlich auf SnapMirror Zielsystemen, um Klone aus dem sekundären SnapMirror Backup zu erstellen.
Protokolle	• ISCSI- oder FC-Lizenz für LUNs • CIFS-Lizenz für SMB-Freigaben • NFS-Lizenz für NFS-Typ VMDKs • ISCSI- oder FC-Lizenz für VMFS-VMDKs des Typs VMDK Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.
SnapCenter-Standardlizenzen (optional)	Sekundäre Ziele Es wird empfohlen, aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standardlizenzen nicht für sekundäre Ziele aktiviert sind, können Sie nach einem Failover-Vorgang SnapCenter nicht für ein Backup von Ressourcen auf dem sekundären Ziel verwenden. Allerdings ist eine FlexClone Lizenz für sekundäre Ziele erforderlich, um Klon- und Verifizierungsvorgänge durchzuführen.

Lizenzen für SnapCenter Advanced- und SnapCenter-NAS-Fileservices sind veraltet und sind nicht mehr verfügbar. Für Amazon FSX for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP und Azure NetApp Files sind die Standardlizenz und die kapazitätsbasierte Lizenz nicht mehr erforderlich.

Sie sollten eine oder mehrere SnapCenter Lizenzen installieren. Informationen zum Hinzufügen von Lizenzen finden Sie unter "Controller-basierte SnapCenter Standard-Lizenzen hinzufügen".

Single Mailbox Recovery-Lizenzen (SMBR

Wenn Sie für das Management von Microsoft Exchange Server Datenbanken und Single Mailbox Recovery (SMBR) mit dem SnapCenter Plug-in für Exchange arbeiten, benötigen Sie eine zusätzliche Lizenz für SMBR, die separat in Abhängigkeit von der Benutzer-Mailbox erworben werden muss.

Die Einstellung der Verfügbarkeit für NetApp Single Mailbox Recovery (EOA) steht am 12. Mai 2023 fest. Weitere Informationen finden Sie unter "CPC-00507". NetApp unterstützt Kunden, die für den Zeitraum der Support-Berechtigung Mailbox-Kapazität, Wartung und Support erworben haben, weiterhin über die am 24. Juni 2020 eingeführten Marketing-Teilenummern.

NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. OnTrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können von Ontrack (bis licensingteam@ontrack.com) neue Ontrack PowerControls Softwarelizenzen und Ontrack PowerControls Wartungs- und Supportverlängerungen für eine granulare Mailbox-Recovery nach dem EOA-Datum vom 12. Mai 2023 beziehen.

Registrieren Sie sich, um auf die SnapCenter Software zuzugreifen

Sie können auf die SnapCenter-Software zugreifen, wenn Sie noch kein NetApp-Konto besitzen und noch kein Amazon FSX for NetApp ONTAP oder Azure NetApp Files-Konto besitzen.

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 für NetApp ONTAP verwenden, sollten Sie die Dateisystem-ID Ihres FSX für ONTAP-Dateisystems haben.

Über diese Aufgabe

Ihre Registrierung unterliegt der Informationsvalidierung und kann bis zu einem Tag dauern, bis ein neues Konto auf der NetApp Support Website (NSS) bestätigt und ein Upgrade durchgeführt wird, damit Sie über den „Gastzugriff“ vollen Zugriff erhalten.

Schritte

1. Klicken Sie hier, https://mysupport.netapp.com/site/user/registration um sich zu registrieren.
2. Geben Sie Ihre Firmen-E-Mail-ID ein, füllen Sie das Captcha aus und akzeptieren Sie die Datenschutzerklärung 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** aus.
   b. Geben Sie im Feld SERIENNUMMER eine der folgenden Werte ein:
      - Azure-Abonnement-ID, wenn Sie Azure NetApp Files verwenden.
      - Dateisystem-ID, wenn Sie Amazon FSX für NetApp ONTAP verwenden.

Sie können ein Ticket https://mysupport.netapp.com/site/help erstellen, wenn Sie während der Registrierung Probleme haben oder den Status kennen.

Authentifizierungsmethoden für Ihre Anmeldedaten

Je nach Anwendung oder Umgebung verwenden Anmeldeinformationen unterschiedliche Authentifizierungsmethoden. Anmeldedaten authentifizieren Benutzer, sodass sie SnapCenter-Vorgänge ausführen können. Zum Installieren von Plug-ins und einem anderen Satz für Datensicherungsvorgänge sollten Sie einen Satz von Anmeldeinformationen erstellen.

Windows Authentifizierung

Die Windows-Authentifizierungsmethode authentifiziert sich gegen Active Directory. Für die Windows-Authentifizierung wird Active Directory außerhalb von SnapCenter eingerichtet. SnapCenter authentifiziert sich ohne zusätzliche Konfiguration. Sie benötigen Windows-Anmeldedaten, um Aufgaben wie das Hinzufügen von Hosts, die Installation von Plug-in-Paketen und die Planung von Jobs auszuführen.

Nicht vertrauenswürdige Domänenauthentifizierung

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

Authentifizierung für lokale Arbeitsgruppen

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen für Benutzer und Gruppen lokaler Arbeitsgruppen. Die Windows-Authentifizierung für Benutzer und Gruppen lokaler Arbeitsgruppen findet zum Zeitpunkt der Erstellung von Windows-Anmeldeinformationen nicht statt, wird jedoch verschoben, bis die Hostregistrierung und andere Hostvorgänge durchgeführt werden.

SQL Server-Authentifizierung

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

Linux-Authentifizierung

Die Linux-Authentifizierungsmethode authentifiziert sich bei einem Linux-Host. Sie benötigen die Linux-Authentifizierung während des ersten Schritts des Hinzufügens des Linux-Hosts und der Remote-Installation des SnapCenter-Plug-ins-Pakets für Linux über die SnapCenter-Benutzeroberfläche.

AIX-Authentifizierung

Die AIX-Authentifizierungsmethode authentifiziert sich gegen einen AIX-Host. Sie benötigen eine AIX-Authentifizierung während des ersten Schritts, in dem Sie den AIX-Host hinzufügen und das SnapCenter Plug-ins Paket für AIX Remote von der SnapCenter-Benutzeroberfläche aus installieren.

Oracle-Datenbankauthentifizierung

Die Oracle-Datenbankauthentifizierung authentifiziert sich anhand einer Oracle-Datenbank. Sie benötigen eine Oracle-Datenbankauthentifizierung, um Vorgänge in der Oracle-Datenbank auszuführen, wenn die Betriebssystemauthentifizierung auf dem Datenbank-Host deaktiviert ist. Daher sollten Sie vor dem Hinzufügen von Oracle-Datenbankberechtigungen einen Oracle-Benutzer in der Oracle-Datenbank mit sysdba-Berechtigungen erstellen.

Oracle ASM Authentifizierung

Die Oracle ASM-Authentifizierungsmethode authentifiziert sich anhand einer Oracle Automatic Storage Management (ASM)-Instanz. Wenn Sie auf die Oracle ASM-Instanz zugreifen müssen und wenn die Betriebssystemauthentifizierung auf dem Datenbank-Host deaktiviert ist, benötigen Sie eine Oracle ASM-Authentifizierung. Daher sollten Sie vor dem Hinzufügen einer Oracle ASM-Berechtigung einen Oracle-Benutzer mit sysasm-Berechtigungen in der ASM-Instanz erstellen.

RMAN-Katalogauthentifizierung

Die Authentifizierungsmethode des RMAN-Katalogs authentifiziert sich mit der Oracle Recovery Manager (RMAN)-Katalogdatenbank. Wenn Sie einen externen Katalogmechanismus konfiguriert und Ihre Datenbank in der Katalogdatenbank registriert haben, müssen Sie die RMAN-Katalogauthentifizierung hinzufügen.

Storage-Verbindungen und Anmeldedaten

Vor Durchführung von Datensicherungsvorgängen sollten Sie die Speicherverbindungen einrichten und die Zugangsdaten hinzufügen, die der SnapCenter-Server und die SnapCenter-Plug-ins verwenden werden.

- **Speicherverbindungen**

  Über die Speicherverbindungen können SnapCenter-Server und SnapCenter-Plug-ins auf den ONTAP-Speicher zugreifen. Zum Einrichten dieser Verbindungen gehört auch die Konfiguration von Funktionen für das AutoSupport- und Ereignismanagement-System (EMS).

- **Anmeldeinformationen**

  - Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe

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

    - *NetBIOS\Benutzername*
    - *Domain FQDN\Benutzername*
    - *Benutzername@upn*
  - Lokaler Administrator (nur für Arbeitsgruppen)

    Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist.

  Das zulässige Format für das Feld Benutzername lautet: *Username*

- Anmeldedaten für einzelne Ressourcengruppen

  Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Multi-Faktor-Authentifizierung (MFA)

Multi-Faktor-Authentifizierung (MFA) managen

Sie können die Multi-Faktor-Authentifizierung (MFA)-Funktion im Active Directory-Verbunddienst (AD FS) und im SnapCenter-Server verwalten.

Multi-Faktor-Authentifizierung (MFA) aktivieren

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

Über diese Aufgabe

- SnapCenter unterstützt SSO-basierte Anmeldungen, wenn andere Applikationen mit demselben AD FS konfiguriert werden. In bestimmten AD FS-Konfigurationen erfordert SnapCenter möglicherweise aus Sicherheitsgründen die Benutzerauthentifizierung in Abhängigkeit von der Persistenz der AD FS-Session.
- Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können und deren Beschreibungen können durch Ausführen abgerufen werden `Get-Help command_name`. Alternativ können Sie auch sehen "SnapCenter Software Cmdlet Referenzhandbuch".

Bevor Sie beginnen

- Der Windows Active Directory Federation Service (AD FS) sollte in der jeweiligen Domäne ausgeführt werden.
- Sie sollten über einen AD FS-unterstützten Multi-Faktor-Authentifizierungsservice wie Azure MFA, Cisco Duo usw. verfügen.
- Der SnapCenter- und AD-FS-Server-Zeitstempel sollte unabhängig von der Zeitzone gleich sein.
- Beschaffung und Konfiguration des autorisierten CA-Zertifikats für den SnapCenter-Server.

  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 bei Upgrade, Reparatur oder Disaster Recovery (DR) in einer Standalone- oder Hochverfügbarkeitskonfiguration das selbstsignierte Zertifikat nicht wiederhergestellt wird, wodurch MFA neu konfiguriert werden kann.
  - Stellt IP-FQDN-Auflösungen sicher.

    Informationen zum CA-Zertifikat finden Sie unter "ZertifikatCSR-Datei erstellen".

Schritte

1. Stellen Sie eine Verbindung zum Active Directory Federation Services (AD FS)-Host her.
2. Laden Sie die AD FS-Verbundmetadaten-Datei von FQDN>/FederationMetadata/2007-06/FederationMetadata.XML herunter "https://<host .“

3. Kopieren Sie die heruntergeladene Datei auf SnapCenter-Server, um die MFA-Funktion zu aktivieren.
4. Melden Sie sich bei SnapCenter Server als SnapCenter-Administrator-Benutzer über PowerShell an.
5. Generieren Sie mithilfe der PowerShell-Sitzung die SnapCenter MFA-Metadatendatei mit dem Cmdlet *New-SmMultifactorAuthenticationMetadata -Path*.

   Der Parameter Path gibt den Pfad an, in dem die MFA-Metadatendatei im SnapCenter-Server-Host gespeichert werden soll.
6. Kopieren Sie die generierte Datei auf den AD FS-Host, um SnapCenter als Client-Einheit zu konfigurieren.
7. Aktivieren Sie MFA für SnapCenter Server mit dem `Set-SmMultiFactorAuthentication` Cmdlet.
8. (Optional) Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mit dem `Get-SmMultiFactorAuthentication` Cmdlet.
9. Gehen Sie zur Microsoft Management Console (MMC), und führen Sie die folgenden Schritte aus:
   a. Klicken Sie Auf **Datei** > **Snapin Hinzufügen/Entfernen**.
   b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
   c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
   d. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Persönlich** > **Zertifikate**.
   e. Klicken Sie mit der rechten Maustaste auf das CA-Zertifikat, das an SnapCenter gebunden ist, und wählen Sie dann **Alle Aufgaben** > **Privater Schlüssel verwalten** aus.
   f. Führen Sie auf dem 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 **Locations** auf **OK**.
      iv. Geben Sie im Feld Objektname 'IIS_IUSRS' ein, und klicken Sie auf **Namen überprüfen** und klicken Sie auf **OK**.

      Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.
10. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie mit der rechten Maustaste auf **vertraut auf Partei** > **Vertrauensbeschuss hinzufügen** > **Start**.
    b. Wählen Sie die zweite Option aus, und 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 eine Zugangskontrollrichtlinie nach Bedarf aus und klicken Sie auf **Weiter**.
    e. Wählen Sie die Einstellungen auf der nächsten Registerkarte standardmäßig aus.
    f. Klicken Sie Auf **Fertig Stellen**.

    SnapCenter wird jetzt als vertrauensanzeige-Partei mit dem angegebenen Anzeigenamen dargestellt.
11. Wählen Sie den Namen aus, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie Auf **Richtlinie Zur Bearbeitung Von Forderungen**.

b. Klicken Sie auf **Regel hinzufügen** und klicken Sie auf **Weiter**.

c. Geben Sie einen Namen für die Antragsregel an.

d. Wählen Sie **Active Directory** als Attributspeicher aus.

e. Wählen Sie das Attribut als **Benutzer-Principal-Name** und den ausgehenden Antragsart als **Name-ID** aus.

f. Klicken Sie Auf **Fertig Stellen**.

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 durch, um zu bestätigen, dass die Metadaten erfolgreich importiert wurden.

a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauensbesteller und wählen Sie **Eigenschaften**.

b. Stellen Sie sicher, dass die Felder Endpoints, Identifikatoren und Signatur ausgefüllt sind.

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

Die SnapCenter MFA-Funktion kann auch über REST-APIs aktiviert werden.

Informationen zur Fehlerbehebung finden Sie unter "Gleichzeitige Anmeldeversuche auf mehreren Registerkarten zeigen MFA-Fehler an".

AD FS MFA-Metadaten aktualisieren

Sie sollten die AD FS MFA-Metadaten in SnapCenter aktualisieren, sobald es Änderungen im AD FS-Server gibt, wie z. B. Upgrade, CA-Zertifikatverlängerung, DR usw.

Schritte

1. Laden Sie die AD FS-Verbundmetadaten-Datei von FQDN>/FederationMetadata/2007-06/FederationMetadata.XML herunter "https://<host .“
2. Kopieren Sie die heruntergeladene Datei auf 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 Session-Cookies zu löschen, und melden Sie sich erneut an.

SnapCenter MFA-Metadaten aktualisieren

Sie sollten die SnapCenter MFA-Metadaten in AD FS immer dann aktualisieren, wenn es Änderungen am ADFS-Server gibt, wie Reparatur, CA-Zertifikatverlängerung, DR usw.

Schritte

1. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
   a. Klicken Sie Auf **Treuhand-Party-Trusts**.
   b. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauensgesellschaft, das für SnapCenter erstellt wurde, und klicken Sie auf **Löschen**.

      Der benutzerdefinierte Name des Vertrauensverhältnisses wird angezeigt.

   c. Multi-Faktor-Authentifizierung (MFA) aktivieren.

      Siehe "Multi-Faktor-Authentifizierung aktivieren".

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

Multi-Faktor-Authentifizierung (MFA) deaktivieren

Schritte

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

Multi-Faktor-Authentifizierung (MFA) mit Rest-API, PowerShell und SCCLI managen

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

Richten Sie AD FS als OAuth/OIDC ein

Konfigurieren Sie AD FS mit dem Windows GUI Wizard

1. Navigieren Sie zu **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Navigieren Sie zu **ADFS** > **Anwendungsgruppen**.
   a. Klicken Sie mit der rechten Maustaste auf **Anwendungsgruppen**.
   b. Wählen Sie **Add Application Group** und geben Sie **Application Name** ein.
   c. Wählen Sie **Server-Anwendung**.
   d. Klicken Sie Auf **Weiter**.
3. Kopieren Sie Die Client-Kennung*.

   Dies ist die Client-ID. .. RückrufURL (SnapCenter-Server-URL) in Umleitung URL hinzufügen. .. Klicken Sie Auf **Weiter**.

4. Wählen Sie **gemeinsam genutzten Schlüssel generieren**.

   Kopieren Sie den geheimen Wert. Das ist das Geheimnis des Kunden. .. Klicken Sie Auf **Weiter**.

5. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.
   a. Klicken Sie auf der Seite **complete** auf **Close**.

6. Klicken Sie mit der rechten Maustaste auf die neu hinzugefügte **Application Group** und wählen Sie **Properties**.
7. Wählen Sie aus den Anwendungseigenschaften **Anwendung hinzufügen**.
8. Klicken Sie auf **Anwendung hinzufügen**.

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

9. Geben Sie auf der Seite WebAPI konfigurieren die im vorherigen Schritt erstellte SnapCenter-Server-URL und die Clientkennung in den Abschnitt Kennung ein.
   a. Klicken Sie Auf **Hinzufügen**.
   b. Klicken Sie Auf **Weiter**.
10. Wählen Sie auf der Seite **Select Access Control Policy** die Kontrollrichtlinie entsprechend Ihrer Anforderung aus (z. B. „Permit everyone“ und „Require MFA“) und klicken Sie auf **Next**.
11. Auf der Seite **Configure Application permission** wird openid standardmäßig als Bereich ausgewählt, klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

    Klicken Sie auf der Seite **complete** auf **Close**.

13. Klicken Sie auf der Seite **Beispielanwendungseigenschaften** auf **OK**.
14. JWT-Token, das von einem Autorisierungsserver (AD FS) ausgegeben und von der Ressource verwendet werden soll.

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

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

    Konfigurieren Sie OpenID Connect so, dass ein Benutzername als Schadensfälle angegeben wird.

16. Öffnen Sie das Tool **AD FS Management** im Menü **Tools** oben rechts im Server Manager.
    a. Wählen Sie in der linken Seitenleiste den Ordner **Anwendungsgruppen** aus.
    b. Wählen Sie die Web-API aus und klicken Sie auf **EDIT**.
    c. Wechseln Sie zur Registerkarte „Emissionsumform“
17. Klicken Sie Auf **Regel Hinzufügen**.
    a. Wählen Sie in der Dropdown-Liste „Antragsregel“ die Option **LDAP-Attribute als Schadensfall senden** aus.
    b. Klicken Sie Auf **Weiter**.
18. Geben Sie den Namen **Claim rule** ein.
    a. Wählen Sie **Active Directory** in der Dropdown-Liste Attributspeicher aus.
    b. Wählen Sie **User-Principal-Name** in der Dropdown-Liste **LDAP Attribute** und **UPN** in der Dropdown-Liste O*utgoing Claim Type* aus.
    c. Klicken Sie Auf **Fertig Stellen**.

Erstellen Sie eine Anwendungsgruppe mit PowerShell Befehlen

Sie können die Anwendungsgruppe und die Web-API erstellen und den Umfang und die Ansprüche mit PowerShell Befehlen hinzufügen. Diese Befehle sind im automatisierten Skriptformat verfügbar. Weitere Informationen finden Sie im <link to KB article>.

1. Erstellen Sie die neue Anwendungsgruppe in AD FS mit der folgenden Kombination.

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

   `ClientRoleIdentifier` Name Ihrer Applikationsgruppe

   `redirectURL` Gültige URL für Umleitung nach Autorisierung

2. Erstellen Sie die AD FS Server-Anwendung und generieren Sie den Client-Schlüssel.

   ```
   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 den Client-Schlüssel aus der Ausgabe der folgenden Befehle, da sie nur einmal angezeigt wird.

   ```
   "client_id = $identifier"

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

5. Erteilen Sie der AD FS-Anwendung die allattallatallaims und openid-Berechtigungen.

   ```
   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 Transformer-Regeldatei aus.

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

7. Benennen Sie die Web-API-Anwendung und definieren Sie die zugehörigen Regeln für die Emissionstransformation mithilfe einer externen Datei.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Ablaufdatum des Zugriffstoken aktualisieren

Sie können die Ablaufzeit des Zugriffstoken mit dem PowerShell Befehl aktualisieren.

Über diese Aufgabe

- Ein Zugriffstoken kann nur für eine bestimmte Kombination von Benutzer, Client und Ressource verwendet werden. Zugriffstoken können nicht widerrufen werden und sind bis zu ihrem Ablauf gültig.
- Standardmäßig beträgt die Gültigkeitsdauer eines Zugriffstoken 60 Minuten. Diese minimale Verfallszeit ist ausreichend und skaliert. Sie müssen ausreichend Wert bieten, um fortlaufende geschäftskritische Aufgaben zu vermeiden.

Schritt

Verwenden Sie den folgenden Befehl im AD FS-Server, um die Ablaufzeit des Zugriffstoken für eine Anwendungsgruppe WebAPI zu aktualisieren.

+

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

Holen Sie sich das Inhabertoken von AD FS

Sie sollten die unten genannten Parameter in jedem REST-Client (wie Postman) ausfüllen und Sie werden aufgefordert, die Benutzeranmeldeinformationen einzugeben. Zusätzlich sollten Sie die zweite-Faktor-Authentifizierung eingeben (etwas, das Sie haben und etwas, das Sie sind), um den Träger-Token zu erhalten.

+ die Gültigkeit des Inhabertoken ist vom AD FS-Server pro Anwendung konfigurierbar und die Standardgültigkeitsdauer beträgt 60 Minuten.

Feld	Wert

Zuteilungsart	Autorisierungscode
Rückruf-URL	Geben Sie die Basis-URL Ihrer Anwendung ein, wenn Sie keine Rückruf-URL haben.
Authentifizs-URL	[adfs-Domain-Name]/adfs/oauth2/Autorisieren
Zugriff auf Token-URL	[adfs-Domain-Name]/adfs/oauth2/Token
Client-ID	Geben Sie die AD FS-Client-ID ein
Kundengeheimnis	Geben Sie den AD FS-Client-Schlüssel ein
Umfang	OpenID
Clientauthentifizierung	Als Basis-AUTH-Kopfzeile senden
Ressource	Fügen Sie auf der Registerkarte **Advance Options** das Ressourcenfeld mit dem gleichen Wert wie die Callback-URL hinzu, das als „aud“-Wert im JWT-Token erscheint.

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

Sie können MFA in SnapCenter-Server mit 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 Trägertoken zur Authentifizierung des Benutzers zu verwenden.

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

Nach Ausführung des oben genannten Cmdlet wird eine Sitzung erstellt, damit der jeweilige Benutzer weitere SnapCenter Cmdlets ausführen kann.

SnapCenter MFA Rest API-Authentifizierung

Verwenden Sie das Trägertoken im Format *Authorization=Bearer <access token>* im REST-API-Client (wie Postman oder swagger) und geben Sie den Benutzer RoleName in der Kopfzeile 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 (Träger) 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 authentifizieren Sie es für nachfolgende Anfragen (SnapCenter Rest API), um einen Vorgang 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 zu erhalten.

   Wenn Sie auf die Schaltfläche klicken, um ein Zugriffstoken für eine Anwendung zu erhalten, werden Sie zur AD FS SSO-Seite weitergeleitet, auf der Sie Ihre AD-Anmeldeinformationen angeben und sich bei 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@Domain oder Domain\user formatiert werden.

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 Konfiguration).
   - Push: Genehmigen Sie die Push-Benachrichtigung, die an Ihr Telefon gesendet wird.
   - QR-Code: Verwenden Sie die mobile App AUTH Point, um den QR-Code zu scannen, und geben Sie dann den in der App angezeigten Verifizierungscode ein
   - Einmalpasswort: Geben Sie das Einmalpasswort für Ihr Token ein.
5. Nach erfolgreicher Authentifizierung wird ein Popup-Fenster geöffnet, das die Token Zugriff, ID und Aktualisieren enthält.

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

6. In der Rest-API sollten Sie das Zugriffstoken und den Rollennamen in der Kopfzeile übergeben.
7. SnapCenter validiert dieses Zugriffstoken aus AD FS.

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

8. Mit dem Benutzernamen und Rollennamen authentifiziert SnapCenter den Benutzer für eine API-Ausführung.

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

Aktivieren oder Deaktivieren der SnapCenter-MFA-Funktion für Rest-API, CLI und GUI

GUI

Schritte

1. Melden Sie sich beim SnapCenter-Server als SnapCenter-Administrator an.

2. Klicken Sie auf **Einstellungen** > **Globale Einstellungen** > **MultiFactorAuthentication(MFA) Settings**
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 zur Aktivierung von MFA für GUI, Rest API, PowerShell und SCCLI aus.

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

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

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

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mit dem `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 zur Aktivierung von MFA für GUI, Rest-API, PowerShell und SCCLI aus.

Parameter	Wert
Angeforderte URL	/API/4.9/settings/multifactorauthentifizierung
HTTP-Methode	Post
Text Anfordern	{ "IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.XML" }

Antwortkörper	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.XML", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }

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

Parameter	Wert
Angeforderte URL	/API/4.9/settings/multifactorauthentifizierung
HTTP-Methode	Verstehen
Antwortkörper	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.XML", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }

Installieren Sie den SnapCenter-Server auf dem Windows-Host

Sie können die ausführbare Datei für das SnapCenter-Server-Installationsprogramm ausführen, um den SnapCenter-Server zu installieren.

Optional können Sie mithilfe von PowerShell Cmdlets mehrere Installations- und Konfigurationsverfahren 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 mit Windows-Updates auf dem neuesten Stand sein, ohne dass das System neu gestartet werden muss.
- Sie sollten sicherstellen, dass MySQL Server nicht auf dem Host installiert ist, auf dem Sie den SnapCenter-Server installieren möchten.
- Sie sollten das Debuggen von Windows-Installateurs aktiviert haben.

  Weitere Informationen zum Aktivieren finden Sie auf der Microsoft-Website "Windows Installer-Protokollierung".

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

Schritte

1. Laden Sie das Installationspaket für den SnapCenter-Server von herunter "NetApp Support-Website".
2. Starten Sie die Installation des SnapCenter-Servers, indem Sie auf die heruntergeladene .exe-Datei doppelklicken.

   Nach Beginn der Installation werden alle Vorabprüfungen durchgeführt und wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

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

3. Überprüfen Sie die für die SnapCenter Server-Installation erforderlichen vordefinierten Werte, und ändern Sie sie, falls erforderlich.

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

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

4. Klicken Sie Auf **Jetzt Installieren**.

   Wenn 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 der Rollback-Vorgang gestartet. Der SnapCenter-Server wird vollständig vom Host entfernt.

   Wenn Sie jedoch **Abbrechen** klicken, wenn die Vorgänge „Neustart des SnapCenter-Servers“ oder „Warten auf Start des SnapCenter-Servers“ ausgeführt werden, wird die Installation ohne Abbrechen des Vorgangs fortgesetzt.

   Protokolldateien werden immer im Ordner %temp% des Admin-Benutzers aufgeführt (älteste zuerst). Wenn Sie die Protokollspeicherorte umleiten möchten, starten Sie die SnapCenter-Serverinstallation über die Eingabeaufforderung, indem Sie Folgendes ausführen:`C:\installer_location\installer_name.exe /log"C:\"`

Registrieren Sie das Produkt, um den Support zu aktivieren

Wenn Sie neue NetApp Produkte nutzen und noch kein NetApp Konto haben, sollten Sie das Produkt registrieren, um den Support zu aktivieren.

Schritte

1. Navigieren Sie nach der Installation von SnapCenter zu **Hilfe > Info**.
2. Notieren Sie sich im Dialogfeld *Info zu SnapCenter* die SnapCenter-Instanz, eine 20-stellige Zahl, die mit 971 beginnt.
3. Klicken Sie Auf https://register.netapp.com.
4. Klicken Sie auf **Ich bin kein registrierter NetApp-Kunde**.

5. Geben Sie Ihre Daten an, um sich zu registrieren.
6. Lassen Sie das Feld NetApp Referenz SN leer.
7. Wählen Sie in der Dropdown-Liste Produktreihe **SnapCenter** aus.
8. Wählen Sie den Abrechnungsanbieter aus.
9. Geben Sie die 20-stellige SnapCenter-Instanz-ID ein.
10. Klicken Sie Auf **Absenden**.

Installieren Sie den SnapCenter-Server auf dem Linux-Host

Sie können die ausführbare Datei für das SnapCenter-Server-Installationsprogramm ausführen, um den SnapCenter-Server zu installieren.

Bevor Sie beginnen

- Wenn Sie den SnapCenter-Server unter Verwendung eines nicht-root-Benutzers installieren möchten, der nicht über ausreichende Berechtigungen zum Installieren von SnapCenter verfügt, rufen Sie die sudoers-Prüfsummendatei von der NetApp-Support-Website ab. Sie sollten die entsprechende Prüfsummendatei verwenden, die auf der Linux-Version basiert.
- Während der Installation von . NET Runtime, wenn die Installation die Abhängigkeiten der *libicu*-Bibliothek nicht auflöst, 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 Befehl ausführen: `yum install -y perl`
- 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 einen Installationsfehler zu vermeiden.
- Überprüfen Sie den sicheren Linux-Status, indem Sie den Befehl ausführen `sestatus`. Wenn der *SELinux Status* „aktiviert“ ist und der *Current Mode* „erzwingt“ ist, führen Sie folgende Schritte aus:
  - Führen Sie den 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 aus `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, in dem Sie Lese- und Schreibberechtigungen haben:
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

      Wenn der Befehl „nichts zu tun“ zurückgibt, führen Sie den Befehl nach der Installation des SnapCenter-Servers 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`

Über diese Aufgabe

- Wenn SnapCenter-Server auf dem Linux-Host installiert ist, werden Dienste von Drittanbietern wie MySQL, RabbitMQ und Errlang 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 Creds)
  - Schlüsselbasierte Authentifizierung zur Anmeldung bei SnapCenter

Schritte

1. Laden Sie Folgendes von */Home Directory* herunter "NetApp Support-Website" .
   - 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. Für die Installation eines nicht-root-Benutzers fügen Sie 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 zur Installation des SnapCenter-Servers durch.

Wenn Sie Folgendes ausführen möchten:	Tun Sie das…
Interaktive Installation	`./snapcenter-linux-server-(el8/el9/sles15).bin` Sie werden aufgefordert, die folgenden Details einzugeben: • Der externe Webapp-Port, der für den Zugriff auf SnapCenter-Server außerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8146. • Der SnapCenter-Server-Benutzer, der den SnapCenter-Server installieren wird. • Das Installationsverzeichnis, in dem Pakete installiert werden.

Wenn Sie Folgendes ausführen möchten:	Tun Sie das…
Nicht interaktive Installation	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` Beispiel: Sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_dir=/opt -DINSTALL_LOG_NAME=InstallerLog.log Protokolle werden unter */var/opt/snapcenter/logs* gespeichert. Zu übergebene Parameter für die Installation des SnapCenter-Servers: • DWEBAPP_EXTERNAL_PORT: Externer Webapp-PORT, der verwendet wird, um außerhalb des Linux-Hosts auf den SnapCenter-Server zuzugreifen. Der Standardwert ist 8146. • DWEBAPP_INTERNAL_PORT: Interner Webapp-PORT, der für den Zugriff auf den SnapCenter-Server innerhalb des Linux-Hosts verwendet wird. Der Standardwert ist 8147. • DSMCORE_PORT: SMCore-Port, auf dem die smcore-Dienste ausgeführt werden. Der Standardwert ist 8145. • DSCHEDULER_PORT: Scheduler-Port, auf dem die Scheduler-Dienste ausgeführt werden. Der Standardwert ist 8154. • DSNAPCENTER_SERVER_USER: SnapCenter-SERVER-Benutzer, der den SnapCenter-Server installieren wird. Bei *DSNAPCENTER_SERVER_USER* ist der Standard der Benutzer, der das Installationsprogramm ausführt. • DUSER_INSTALL_dir: Installationsverzeichnis, in dem Pakete installiert werden. Für *DUSER_INSTALL_dir* lautet das Standardinstallationsverzeichnis */opt*. • DINSTALL_LOG_NAME: NAME der Protokolldatei, in der die Installationsprotokolle gespeichert werden. Dies ist ein optionaler Parameter, und wenn angegeben, werden keine Protokolle auf der Konsole angezeigt. Wenn Sie diesen Parameter nicht angeben, werden

Was kommt als Nächstes?

- Wenn der *SELinux Status* "aktiviert" ist und der *Current Mode* "erzwingt" ist, startet der **nginx**-Dienst nicht. Sie sollten die folgenden Befehle ausführen:
  a. Gehen Sie zum Home Directory.
  b. Führen Sie den Befehl aus: `journalctl -x|grep nginx`.
  c. Wenn der interne Webapp-Port (8147) nicht hören darf, führen Sie die folgenden Befehle aus:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Lauf `setsebool -P httpd_can_network_connect on`

Protokolle auf der Konsole angezeigt und auch in der Standardprotokolldatei gespeichert.

- DSELINUX: Wenn *SELinux Status* "aktiviert" ist, ist der *Current Mode* "Enforcing" und Sie haben die Befehle ausgeführt, die im Abschnitt vor dem Start erwähnt wurden, sollten Sie diesen Parameter angeben und den Wert als 1 zuweisen. Der Standardwert ist 0.
- DUPGRADE: Der Standardwert ist 0. Geben Sie diesen Parameter und seinen Wert als eine ganze Zahl außer 0 an, um den SnapCenter-Server zu aktualisieren.

Registrieren Sie das Produkt, um den Support zu aktivieren

Wenn Sie zum ersten mal bei NetApp sind und noch kein NetApp Konto haben, sollten Sie das Produkt registrieren, um den Support zu aktivieren.

Schritte

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

Melden Sie sich über die RBAC-Autorisierung bei SnapCenter an

SnapCenter unterstützt die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC). Der SnapCenter Administrator weist über die SnapCenter RBAC Rollen und Ressourcen entweder einem Benutzer in der Arbeitsgruppe oder im aktiven Verzeichnis oder Gruppen im aktiven Verzeichnis zu. Der RBAC-Benutzer kann sich nun mit den zugewiesenen Rollen bei SnapCenter anmelden.

Bevor Sie beginnen

- Sie sollten den Windows Process Activation Service (WAR) in Windows Server Manager aktivieren.
- Wenn Sie Internet Explorer als Browser verwenden möchten, um sich beim SnapCenter-Server anzumelden, sollten Sie sicherstellen, dass der geschützte Modus in Internet Explorer deaktiviert ist.
- Wenn SnapCenter-Server auf Linux-Host installiert ist, sollten Sie sich mit dem Benutzerkonto anmelden, das zur Installation des SnapCenter-Servers verwendet wurde.

Über diese Aufgabe

Während der Installation erstellt der Installationsassistent für SnapCenter-Server eine Verknüpfung und legt sie auf dem Desktop und im Startmenü des Hosts ab, auf dem SnapCenter installiert ist. Außerdem 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, meldet Sie sich beim Schließen der Registerkarte „SnapCenter-Browser“ nicht von SnapCenter ab. Um Ihre Verbindung mit SnapCenter zu beenden, müssen Sie sich von SnapCenter entweder durch Klicken auf den **Abmelden**-Button oder durch Schließen des gesamten Webbrowsers abmelden.

Best Practice: aus Sicherheitsgründen wird empfohlen, dass Sie Ihren Browser nicht aktivieren, um 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 Server-Port bereitgestellt haben, wird dieser Port verwendet.

Für die Bereitstellung von Hochverfügbarkeit (HA) müssen Sie mithilfe der virtuellen Cluster-IP_\https://Virtual_Cluster_IP_or_FQDN:8146_. auf SnapCenter zugreifen Wenn die SnapCenter-Benutzeroberfläche beim Navigieren zu *https://Virtual_Cluster_IP_or_FQDN:8146* im Internet Explorer (IE) nicht angezeigt wird, müssen Sie die IP-Adresse oder den FQDN des virtuellen Clusters als vertrauenswürdige Site in IE auf jedem Plug-in-Host hinzufügen, oder Sie müssen die erweiterte Sicherheit von IE auf jedem Plug-in-Host deaktivieren. Weitere Informationen finden Sie unter "Der Zugriff auf die Cluster-IP-Adresse kann nicht vom externen Netzwerk aus erfolgen".

Über die SnapCenter GUI hinaus können Sie mit PowerShell Cmdlets Skripte erstellen, um Konfigurations-, Backup- und Restore-Vorgänge durchzuführen. Einige Cmdlets haben sich möglicherweise bei jeder SnapCenter Version geändert. Das "SnapCenter Software Cmdlet Referenzhandbuch" 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 Hostdesktop, über die am Ende der Installation angegebene URL oder über die vom SnapCenter-Administrator bereitgestellte URL.
2. Geben Sie die Anmeldedaten des Benutzers ein.

So geben Sie Folgendes an:	Verwenden Sie eines dieser Formate…
Domain-Administrator	• NetBIOS\Benutzername • Benutzername@UPN-Suffix Beispiel: username@netapp.com • Domain FQDN\Benutzername

So geben Sie Folgendes an:	Verwenden Sie eines dieser Formate…
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.

   Ihre aktuellen Benutzer und die zugehörige Rolle werden nach der Anmeldung oben rechts von SnapCenter angezeigt.

Ergebnis

Die Seite Dashboard wird angezeigt.

Wenn die Protokollierung mit dem Fehler fehlschlägt, dass die Site nicht erreicht werden kann, sollten Sie das SSL-Zertifikat SnapCenter zuordnen. "Weitere Informationen ."

Nach Ihrer Beendigung

Nachdem Sie sich zum ersten Mal bei SnapCenter Server als RBAC-Benutzer angemeldet haben, aktualisieren Sie die Ressourcenliste.

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. "Weitere Informationen .".

Wenn Sie den Plug-in-Host in SnapCenter unter Linux Host hinzufügen möchten, sollten Sie die Prüfsummendatei vom Speicherort abrufen: */opt/NetApp/snapManagerWeb/Repository*.

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

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

SnapCenter Server unterstützt MFA für Domain-Konto, das Teil des Active Directory ist.

Bevor Sie beginnen

Sie sollten MFA aktiviert haben. Informationen zum Aktivieren von MFA finden Sie unter "Multi-Faktor-Authentifizierung aktivieren"

Über diese Aufgabe

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

Schritte

1. Starten Sie SnapCenter über die Verknüpfung auf Ihrem lokalen Hostdesktop, über die am Ende der Installation angegebene URL oder über die vom SnapCenter-Administrator bereitgestellte URL.
2. Geben Sie auf der Anmeldeseite AD FS Benutzernamen und Kennwort ein.

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

- Gibt an, ob Benutzername oder Passwort gültig ist

  Das Benutzerkonto sollte im Active Directory (AD) vorhanden sein.

- Ob Sie die maximal zulässigen Versuche überschritten haben, die in AD festgelegt wurden
- Gibt an, ob AD und AD FS verfügbar ist und ausgeführt wird

Ändern Sie das Zeitlimit für die SnapCenter-StandardGUI-Sitzung

Sie können den Zeitlimits für die SnapCenter-GUI-Sitzung ändern, damit sie kürzer als oder größer als der Standardzeitraum von 20 Minuten ist.

Als Sicherheitsfunktion warnt Sie SnapCenter nach einer Standardlaufzeit 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 Session-Timeout die neue Sitzungszeitüberschreitung in Minuten ein und klicken Sie dann auf **Speichern**.

Sichern Sie den SnapCenter Webserver durch Deaktivieren von SSL 3.0

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

Das SSL 3.0-Protokoll enthält Mängel, mit denen ein Angreifer Verbindungsfehler verursachen kann oder man-in-the-Middle-Angriffe ausführen und den Verschlüsselungsverkehr zwischen Ihrer Website und ihren Besuchern beobachten kann.

Schritte

1. Um den Registrierungs-Editor auf dem SnapCenter-Webserver-Host zu starten, klicken Sie auf **Start** > **Ausführen** und geben dann regedit ein.
2. Navigieren Sie im Registrierungs-Editor zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Falls der Server-Schlüssel 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 Server-Schlüssel nicht vorhanden ist:
     i. Klicken Sie auf **Bearbeiten** > **Neu** > **Schlüssel** und benennen Sie den Schlüssel Server.
     ii. Wenn der neue Serverschlüssel ausgewählt ist, klicken Sie auf **Bearbeiten** > **Neu** > **DWORD**.
     iii. Benennen Sie die neue DWORD aktiviert, und geben Sie dann 0 als Wert ein.
3. Schließen Sie Den Registrierungs-Editor.

Konfigurieren Sie das CA-Zertifikat für den Windows-Host

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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 ein CA-Zertifikat mit SnapCenter Site

Sie sollten das CA-Zertifikat mit der SnapCenter-Site auf einem 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** > **Website 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-Serverhosts, und es ist nicht zwingend erforderlich, mit einem CA-Zertifikat zu konfigurieren. Wenn Sie in Ihrer Umgebung jedoch die Verwendung eines CA-Zertifikats vorschreibt, wiederholen Sie die Schritte 5 bis 9 mithilfe des SnapCenter-Planerstandorts.

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 Sie CA-Zertifikate 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.

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

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **CA Zertifikateinstellungen**.
2. Wählen Sie **Zertifikatvalidierung Aktivieren**.
3. Klicken Sie Auf **Anwenden**.

Nach Ihrer Beendigung

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass kein CA-Zertifikat aktiviert oder dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Konfigurieren Sie das CA-Zertifikat 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 nginx Reverse Proxy, Audit-Protokollierung und 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 Abschnitt Server in der Konfigurationsdatei.
4. Ändern Sie die Pfade von *ssl_Certificate* und *ssl_Certificate_Key*, um auf das CA-Zertifikat zu verweisen.
5. Speichern und schließen Sie die Datei.
6. Nginx neu laden: `$nginx -s reload`

Konfigurieren Sie das Audit-Protokoll-Zertifikat

Schritte

1. Öffnen Sie *INSTALL_dir/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config* mithilfe von 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-Zertifikatspfad und das Passwort einzuschließen.

   Für das Auditprotokoll-Zertifikat wird nur das *.pfx*-Format unterstützt.

3. Speichern und schließen Sie die Datei.
4. Starten Sie den Dienst **SnapManager Web** neu: `$ systemctl restart snapmanagerweb`

Konfigurieren Sie das Zertifikat für SnapCenter-Services

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-Zertifikatspfad und das entsprechende Passwort einzuschließen.

Für das SnapCenter-Servicezertifikat 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 Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Windows-Host

Sie sollten die bidirektionale SSL-Kommunikation so konfigurieren, dass die gegenseitige Kommunikation zwischen SnapCenter-Server auf Windows-Host und den Plug-ins gesichert ist.

Bevor Sie beginnen

- Sie sollten die CSR-Datei des CA-Zertifikats mit der unterstützten Mindestschlüssellänge von 3072 erstellt haben.
- Das CA-Zertifikat sollte die Serverauthentifizierung und die Clientauthentifizierung unterstützen.
- Sie sollten über ein CA-Zertifikat mit privatem Schlüssel und Fingerabdruck-Details verfügen.
- Sie sollten die Einweg-SSL-Konfiguration aktiviert haben.

  Weitere Informationen 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 für die bidirektionale SSL-Kommunikation nicht aktiviert sind, werden nicht unterstützt.

Schritte

1. Um den Port zu binden, führen Sie die folgenden Schritte auf dem SnapCenter-Server-Host für SnapCenter IIS-Webserver-Port 8146 (Standard) und erneut für SMCore-Port 8145 (Standard) mit PowerShell-Befehlen durch.

   a. Entfernen Sie die vorhandene selbstsignierte SnapCenter-Zertifikatport-Bindung mit dem folgenden PowerShell Befehl.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      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 beschaffte 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>
```

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 das CA-Zertifikat zuzugreifen, fügen Sie den Standard-IIS-Webserver-Benutzer „**IIS AppPool\SnapCenter**“ von SnapCenter in die Zertifikatsberechtigungsliste ein, indem Sie die folgenden Schritte ausführen, um auf das neu beschaffte CA-Zertifikat zuzugreifen.
   a. Rufen Sie die Microsoft Management Console (MMC) auf, und klicken Sie dann auf **Datei** > **SnapIn hinzufügen/entfernen**.
   b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
   c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
   d. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Persönlich** > **Zertifikate**.
   e. Wählen Sie das SnapCenter-Zertifikat aus.
   f. Um den Assistenten zum Hinzufügen von Benutzerberechtigungen zu starten\, klicken Sie mit der rechten Maustaste auf das CA-Zertifikat und wählen **Alle Aufgaben** > **Private Schlüssel verwalten**.
   g. Klicken Sie auf **Hinzufügen**, im Assistenten Benutzer und Gruppen auswählen ändern Sie den Speicherort in den lokalen Computernamen (ganz oben in der Hierarchie)
   h. Fügen Sie den Benutzer IIS AppPool\SnapCenter hinzu, geben Sie die vollen Kontrollberechtigungen ein.
3. Fügen Sie für die IIS-Berechtigung **CA-Zertifikat** den neuen DWORD-Registrierungsschlüssel-Eintrag im SnapCenter-Server über den folgenden Pfad hinzu:

Im Windows-Registrierungs-Editor, Traverse auf den unten genannten Pfad,

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
ders\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 aus (Standard).

   a. Entfernen Sie die vorhandene selbstsignierte SnapCenter-Zertifikatport-Bindung mit dem folgenden PowerShell Befehl.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
   ```

   Beispiel:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145
   ```

   b. Binden Sie das neu beschaffte 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>
   ```

   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 Windows-Hosts und den Plug-ins mithilfe von PowerShell-Befehlen zu sichern.

Bevor Sie beginnen

Führen Sie die Befehle für alle Plug-ins und den SMCore-Agent zuerst 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 Agenten aus, für den 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 IIS-SnapCenter-Anwendungspool-Recyclingvorgang 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 die Befehle für alle Plug-ins und den SMCore-Agent zuerst und dann für den Server aus.
- Wenn Sie die bidirektionale SSL-Kommunikation deaktivieren, werden das CA-Zertifikat und seine Konfiguration nicht entfernt.
- Um dem SnapCenter-Server einen neuen Host hinzuzufügen, müssen Sie die bidirektionale SSL-Verbindung 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 IIS-SnapCenter-Anwendungspool-Recyclingvorgang 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 Sie die bidirektionale 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 SnapCenter-Server auf 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 in die Vertrauensliste Ihres Linux-Hosts ein.
   - `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 GUI-Link des SnapCenter-Servers.
6. Aktualisieren Sie die Werte der folgenden Schlüssel in **SnapManager.Web.UI.dll.config** unter _ /<installation path>/NetApp/snapcenter/SnapManagerWeb_ und **SMCoreServiceHost.dll.config** unter

/<installation path>/NetApp/snapcenter/SMCore.

- <add key="SERVICE_CERTIFICATE_PATH" value="<path of 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. Vergewissern Sie sich, dass das Zertifikat an den SnapManager-Webport angeschlossen ist.
   `openssl s_client -connect localhost:8146 -brief`
9. Vergewissern Sie sich, dass das Zertifikat an den smcore-Port angeschlossen ist.
   `openssl s_client -connect localhost:8145 -brief`
10. Kennwort für SPL-Keystore und Alias verwalten.
    a. Rufen Sie das SPL-Keystore-Standardpasswort ab, das dem Schlüssel **SPL_KEYSTORE_PASS** in der SPL-Eigenschaftsdatei zugewiesen wurde.
    b. Ändern Sie das Passwort für den Keystore.
       `keytool -storepasswd -keystore keystore.jks`
    c. Ändern Sie das Passwort für alle Aliase von privaten Schlüsseleinträgen.
       `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 Plug-in-Linux-Host die Root- und Zwischenzertifikate im Keystore 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 Alias 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 **Certificate.pfx**, der in *keystore.jks* gespeichert ist, und starten Sie den SPL-Dienst neu: `systemctl restart spl`
13. Vergewissern Sie sich, dass das Zertifikat an den smcore-Port angeschlossen ist.
    `openssl s_client -connect localhost:8145 -brief`

Aktivieren Sie die SSL-Kommunikation auf Linux-Host

Sie können bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige Kommunikation zwischen SnapCenter Server auf Linux-Host und den Plug-ins mithilfe

von PowerShell-Befehlen zu sichern.

Schritt

1. Führen Sie die folgenden Schritte aus, um die einfache 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 dem SnapCenter-Server aktivieren**.
   c. Klicken Sie auf **Hosts** > **verwaltete Hosts** und wählen Sie den Plug-in-Host aus, für den Sie One-Way-SSL aktivieren möchten.
   d. Klicken Sie auf  , 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 Sie die zertifikatbasierte Authentifizierung

Exportieren Sie Zertifikate der Zertifizierungsstelle (CA) vom SnapCenter-Server

Sie sollten die CA-Zertifikate über die Microsoft Management Console (MMC) vom SnapCenter-Server auf die Plug-in-Hosts exportieren.

Bevor Sie beginnen

Sie sollten die bidirektionale SSL-Konfiguration vorgenommen haben.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster Zertifikate Snap-in die Option **Computerkonto** aus 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 den SnapCenter-Server verwendet wird, und wählen Sie dann **Alle Aufgaben** > **Export** aus, um den Export-Assistenten zu starten.
6. Führen Sie die folgenden Aktionen im Assistenten aus.

Für diese Option…	Gehen Sie wie folgt vor…
Privaten Schlüssel Exportieren	Wählen Sie **Nein, exportieren Sie den privaten Schlüssel nicht**, und klicken Sie dann auf **Weiter**.
Dateiformat Exportieren	Klicken Sie Auf **Weiter**.
Dateiname	Klicken Sie auf **Browse** und geben Sie den Dateipfad an, um das Zertifikat zu speichern, und klicken Sie auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Export zu starten.

Die zertifikatbasierte Authentifizierung wird für SnapCenter HA-Konfigurationen und das SnapCenter Plug-in für VMware vSphere nicht unterstützt.

Zertifikat der Zertifizierungsstelle (CA) auf die Windows-Plug-in-Hosts importieren

Um das exportierte SnapCenter-Server-CA-Zertifikat zu verwenden, sollten Sie das zugehörige Zertifikat über die Microsoft-Managementkonsole (MMC) auf die SnapCenter-Windows-Plug-in-Hosts importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Fenster Zertifikate Snap-in die Option **Computerkonto** aus 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 „Personal“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Import-Assistenten zu starten.
6. Führen Sie die folgenden Aktionen im Assistenten aus.

Für diese Option…	Gehen Sie wie folgt vor…
Speicherort Des Geschäfts	Klicken Sie Auf **Weiter**.
Zu importierende Datei	Wählen Sie das SnapCenter-Serverzertifikat aus, das mit der Erweiterung .cer endet.
Zertifikatspeicher	Klicken Sie Auf **Weiter**.

Für diese Option…	Gehen Sie wie folgt vor…
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Importieren Sie das CA-Zertifikat in die UNIX-Host-Plug-ins, und konfigurieren Sie Root- oder Zwischenzertifikate in den SPL-Trust-Store

Importieren Sie das CA-Zertifikat auf die UNIX-Plug-in-Hosts

Sie sollten das CA-Zertifikat auf die UNIX-Plug-in-Hosts importieren.

Über diese Aufgabe

- Sie können das Kennwort für den SPL-Keystore und den Alias des CA-Schlüsselpaars verwalten, das gerade verwendet wird.
- Das Passwort für den SPL-Keystore und für das zugehörige Alias-Passwort des privaten Schlüssels muss identisch sein.

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen. Es ist der Wert, der der Taste entspricht `SPL_KEYSTORE_PASS`.
2. Ändern Sie das Passwort für den Keystore:
   `$ keytool -storepasswd -keystore keystore.jks`
3. Ändern Sie das Passwort für alle Aliase von privaten Schlüsseleinträgen im Keystore auf dasselbe Passwort, das für den Keystore verwendet wird:
   `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Aktualisieren Sie dasselbe für den Schlüssel SPL_KEYSTORE_PASS in der `spl.properties` Datei.
5. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate für den SPL-Vertrauensspeicher konfigurieren. Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Keystore 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 <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`

5. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder Zwischenzertifikate in den SPL Trust-Store konfiguriert haben.

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

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

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Keystore 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. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Standard-SPL-Keystore-Passwort ist der Wert des Schlüssels SPL_KEYSTORE_PASS in der `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 "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher, der sich in der Datei befindet `spl.properties` . Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.
10. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Aktivieren Sie die zertifikatbasierte Authentifizierung

Führen Sie das folgende PowerShell-Cmdlet aus, um die zertifikatbasierte Authentifizierung für SnapCenter Server und die Windows Plug-in-Hosts zu aktivieren. Bei Linux-Plug-in-Hosts wird die zertifikatbasierte Authentifizierung aktiviert, wenn Sie die bidirektionale SSL-Funktion aktivieren.

- So aktivieren Sie die clientzertifikatbasierte Authentifizierung:

  `Set-SmConfigSettings -Agent –configSettings`

```
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- So deaktivieren Sie die clientzertifikatbasierte Authentifizierung:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Exportieren von SnapCenter-Zertifikaten

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snap-in hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Mein Benutzerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate - Aktueller Benutzer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf das Zertifikat mit dem SnapCenter Friendly Name, und wählen Sie dann **Alle Aufgaben** > **Exportieren** aus, um den Exportassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Exportieren	Wählen Sie die Option **Ja, exportieren Sie den privaten Schlüssel** und klicken Sie dann auf **Weiter**.
Dateiformat Exportieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Zu exportierende Datei	Geben Sie einen Dateinamen für das exportierte Zertifikat an (Sie müssen .pfx verwenden), und klicken Sie dann auf **Weiter**.
Assistent zum Exportieren von Zertifikaten abschließen	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Export zu starten.

Ergebnis

Zertifikate werden im .pfx-Format exportiert.

Konfiguration von Active Directory, LDAP und LDAPS

Registrieren Sie nicht vertrauenswürdige 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 über das LDAP- oder LDAPS-Protokoll registrieren.
- Sie sollten die bidirektionale Kommunikation zwischen den Plug-in-Hosts und dem SnapCenter-Server aktivieren.
- Die DNS-Auflösung sollte vom SnapCenter-Server zu den Plug-in-Hosts eingerichtet und umgekehrt werden.

LDAP-Protokoll

- Der vollständig qualifizierte Domänenname (FQDN) sollte vom SnapCenter-Server resolable sein.

  Sie können eine nicht vertrauenswürdige Domäne mit dem FQDN registrieren. Wenn der FQDN nicht vom SnapCenter-Server aus lösbar ist, können Sie sich mit einer IP-Adresse des Domänencontrollers registrieren, und dieser sollte vom SnapCenter-Server aus gelöst werden können.

LDAPS-Protokoll

- CA-Zertifikate sind für LDAPS erforderlich, um während der Active Directory-Kommunikation eine End-to-End-Verschlüsselung bereitzustellen.

  "Konfigurieren Sie das CA-Client-Zertifikat für LDAPS"

- Domänencontroller Host-Namen (DCHostName) sollten über den SnapCenter Server 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 Sie hier + , 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 für die Registrierung der nicht vertrauenswürdigen Domain für LDAP erforderlich sind:

Für dieses Feld…	Tun Sie das…
Domain-Name	Geben Sie den NetBIOS-Namen für die Domäne an.
Domain-FQDN	Geben Sie den FQDN an und klicken Sie auf **Auflösen**.
IP-Adressen des Domänencontrollers	Wenn der Domain-FQDN nicht vom SnapCenter-Server resolbar ist, geben Sie eine oder mehrere IP-Adressen für den Domänencontroller an. Weitere Informationen finden Sie unter "Fügen Sie von der GUI eine Domänen-Controller-IP für eine nicht vertrauenswürdige Domäne hinzu".

b. Wenn Sie **LDAPS** auswählen, geben Sie die Informationen an, die für die Registrierung der nicht vertrauenswürdigen Domain für LDAPS erforderlich sind:

Für dieses Feld…	Tun Sie das…
Domain-Name	Geben Sie den NetBIOS-Namen für die Domäne an.
Domain-FQDN	Geben Sie den FQDN an.
Domänen-Controller-Namen	Geben Sie einen oder mehrere Domänencontroller-Namen an und klicken Sie auf **Auflösen**.
IP-Adressen des Domänencontrollers	Wenn die Domänencontrollernamen nicht vom SnapCenter-Server behoben werden können, sollten Sie die DNS-Auflösungen beheben.

6. Klicken Sie auf **OK**.

Konfigurieren Sie das CA-Client-Zertifikat für LDAPS

Sie sollten das CA-Clientzertifikat für LDAPS auf dem SnapCenter-Server konfigurieren, wenn die Windows Active Directory-LDAPS mit den CA-Zertifikaten konfiguriert ist.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.

4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Auf der zweiten Seite des Assistenten	Klicken Sie auf **Durchsuchen**, wählen Sie das *Root-Zertifikat* und klicken Sie auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

7. Wiederholen Sie die Schritte 5 und 6 für die Zwischenzertifikate.

Konfiguration Der Hochverfügbarkeit

Konfigurieren Sie SnapCenter-Server für Hochverfügbarkeit

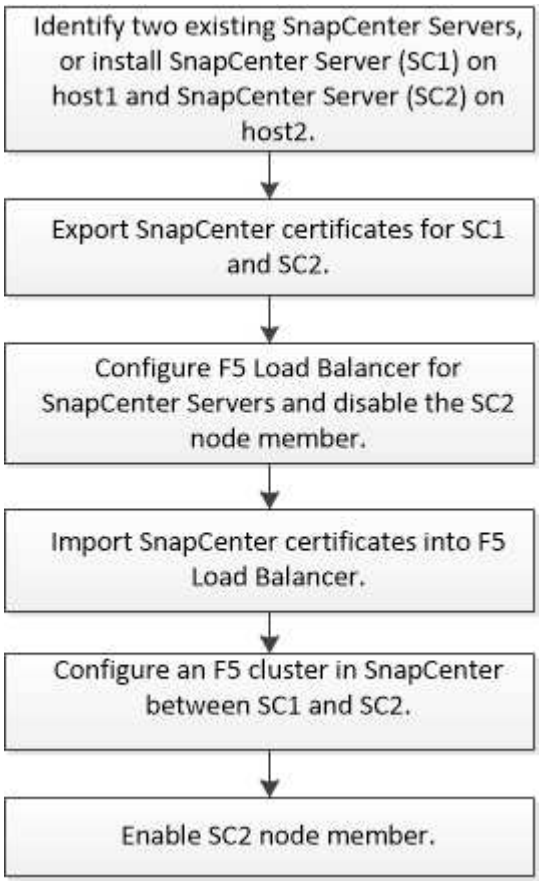
Um Hochverfügbarkeit (HA) in SnapCenter zu unterstützen, die entweder unter Windows oder unter Linux ausgeführt werden, können Sie den F5 Load Balancer installieren. Mit F5 kann der SnapCenter Server aktiv/Passiv-Konfigurationen in bis zu zwei Hosts an demselben Standort unterstützen. Um F5 Load Balancer in SnapCenter zu verwenden, sollten Sie die SnapCenter-Server konfigurieren und F5 Load Balancer konfigurieren.

Sie können auch den Netzwerklastenausgleich (NLB) konfigurieren, um die hohe Verfügbarkeit von SnapCenter einzurichten. Sie sollten NLB außerhalb der SnapCenter-Installation manuell konfigurieren, um eine hohe Verfügbarkeit zu gewährleisten.

Für Cloud-Umgebungen können Sie Hochverfügbarkeit entweder mit Amazon Web Services (AWS) Elastic Load Balancing (ELB) und Azure Load Balancer konfigurieren.

Konfigurieren Sie Hochverfügbarkeit mit F5

Das Workflow-Image führt die Schritte für die Konfiguration von SnapCenter-Servern für hohe Verfügbarkeit mit F5 Load Balancer auf. Ausführliche Anweisungen finden Sie unter "Konfigurieren von SnapCenter-Servern für Hochverfügbarkeit mit F5 Load Balancer".



Sie müssen Mitglied der Gruppe Lokale Administratoren auf den SnapCenter-Servern sein (zusätzlich zur SnapCenterAdmin-Rolle zugewiesen), um die folgenden Cmdlets zum Hinzufügen und Entfernen von F5-Clustern zu verwenden:

- Add-SmServerCluster
- Add-SmServer
- Entfernen Sie-SmServerCluster

  Weitere Informationen finden Sie unter "SnapCenter Software Cmdlet Referenzhandbuch".

Weitere Informationen

- Nachdem Sie SnapCenter für Hochverfügbarkeit installiert und konfiguriert haben, bearbeiten Sie die SnapCenter Desktop-Verknüpfung, um auf die F5 Cluster-IP zu verweisen.
- Wenn ein Failover zwischen SnapCenter-Servern auftritt und es auch eine SnapCenter-Sitzung gibt, müssen Sie den Browser schließen und sich erneut bei SnapCenter anmelden.
- Wenn Sie im Load Balancer Setup (NLB oder F5) einen Host hinzufügen, der teilweise vom NLB- oder F5-Host aufgelöst wurde, und wenn der SnapCenter-Host nicht in der Lage ist, auf diesen Host zuzugreifen, schaltet die SnapCenter-Hostseite häufig zwischen Hosts aus und wird ausgeführt. Um dieses Problem zu beheben, sollten Sie sicherstellen, dass beide SnapCenter-Hosts den Host im

NLB- oder F5-Host lösen können.

- SnapCenter-Befehle für MFA-Einstellungen sollten auf allen Hosts ausgeführt werden. Die Konfiguration von Drittanbieterkonfigurationen sollte auf dem Active Directory Federation Services (AD FS)-Server unter Verwendung von F5-Clusterdetails erfolgen. Der Zugriff auf die SnapCenter-Benutzeroberfläche auf Hostebene wird blockiert, nachdem MFA aktiviert wurde.
- Während des Failovers werden die Einstellungen des Überwachungsprotokolls nicht auf dem zweiten Host wiedergegeben. Daher sollten Sie die Einstellungen des Überwachungsprotokolls auf dem passiven F5-Host manuell wiederholen, wenn er aktiv wird.

Konfigurieren von Hochverfügbarkeit mit Network Load Balancing (NLB)

Sie können den Netzwerklastenausgleich (NLB) konfigurieren, um die hohe Verfügbarkeit von SnapCenter einzurichten. Sie sollten NLB außerhalb der SnapCenter-Installation manuell konfigurieren, um eine hohe Verfügbarkeit zu gewährleisten.

Informationen zum Konfigurieren des Netzwerklastausgleichs (NLB) mit SnapCenter finden Sie unter "So konfigurieren Sie NLB mit SnapCenter".

Hochverfügbarkeit mit AWS Elastic Load Balancing (ELB) konfigurieren

Um eine hochverfügbare SnapCenter-Umgebung in Amazon Web Services (AWS) zu konfigurieren, lassen sich zwei SnapCenter-Server in separaten Verfügbarkeitszonen einrichten und 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 Sie die virtuelle private Overlay-IP".
2. Bereiten Sie Ihren Windows-Host vor
   a. IPv4-Priorität über IPv6 erzwingen:
      - Standort: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameter
      - Schlüssel: DisabledComponents
      - Geben Sie „REG_DWORD“ ein
      - Wert: 0x20
   b. Stellen Sie sicher, dass die vollständig qualifizierten Domänennamen per DNS oder über die lokale Hostkonfiguration an die IPv4-Adressen aufgelöst werden können.
   c. Stellen Sie sicher, dass kein System-Proxy konfiguriert ist.
   d. Stellen Sie sicher, dass das Administratorkennwort auf dem Windows-Server identisch ist, wenn Sie ein Setup ohne Active Directory verwenden und sich die Server nicht in einer Domäne befinden.
   e. Fügen Sie virtuelle IP auf beiden Windows-Servern hinzu.
3. Erstellen Sie den SnapCenter-Cluster.
   a. Starten Sie PowerShell und stellen Sie eine Verbindung mit 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. Erfahren Sie mehr zur Hochverfügbarkeit.
```
Get-SmServerConfig
```

4. Erstellen Sie die Lamda-Funktion, um die Routing-Tabelle anzupassen, falls der virtuelle private IP-Endpunkt nicht mehr verfügbar ist und von AWS CloudWatch überwacht wird. Weitere Informationen finden Sie unter "Lambda-Funktion erstellen".
5. Erstellen Sie einen Monitor in CloudWatch, um die Verfügbarkeit des SnapCenter-Endpunkts zu überwachen. Ein Alarm ist so konfiguriert, dass er eine Lambda-Funktion auslöst, wenn der Endpunkt nicht erreichbar ist. Die Lambda-Funktion passt die Routingtabelle an, um den Datenverkehr auf den aktiven SnapCenter-Server umzuleiten. Weitere Informationen finden Sie unter "Erstellen Sie synthetische Kanaren".
6. Implementieren Sie einen Workflow mit einer Step-Funktion als Alternative zur CloudWatch-Überwachung und profitieren Sie von geringeren Failover-Zeiten. Der Workflow beinhaltet eine Lambda-Sondenfunktion zum Testen der SnapCenter-URL, eine DynamoDB-Tabelle zum Speichern der Fehleranzahl und die Step-Funktion selbst.
   a. Verwenden Sie eine Lambda-Funktion zum Sondieren der SnapCenter-URL. Weitere Informationen finden Sie unter "Lambda-Funktion erzeugen".
   b. Erstellen Sie eine DynamoDB-Tabelle zum Speichern der Fehleranzahl zwischen zwei-Schritt-Funktions-Iterationen. Weitere Informationen finden Sie unter "Erste Schritte mit der DynamoDB-Tabelle".
   c. Erstellen Sie die Step-Funktion. Weitere Informationen finden Sie unter "Dokumentation der Step-Funktion".
   d. Testen Sie einen einzelnen Schritt.
   e. Testen Sie die vollständige Funktion.
   f. IAM-Rolle erstellen und Berechtigungen anpassen, um die Lambda-Funktion ausführen zu dürfen.
   g. Erstellen Sie einen Zeitplan, um die Schrittfunktion auszulösen. Weitere Informationen finden Sie unter "Verwenden des Amazon EventBridge Scheduler zum Starten von Schrittfunktionen".

Konfigurieren Sie Hochverfügbarkeit mit dem Azure Load Balancer

Sie können die SnapCenter-Umgebung mit Hochverfügbarkeit mit dem Azure Load Balancer konfigurieren.

Schritte

1. Erstellen Sie mit dem Azure-Portal Virtual Machines in einem Scale-Set. Mit dem Scale-Set für virtuelle Azure-Maschinen können Sie eine Gruppe von Virtual Machines mit Lastausgleich erstellen und managen. Die Anzahl der virtuellen Maschineninstanzen kann sich automatisch auf die Nachfrage oder einen definierten Zeitplan erhöhen oder verringern. Weitere Informationen finden Sie unter "Erstellen Sie mit dem Azure-Portal Virtual Machines in einem Scale-Set".
2. Melden Sie sich nach dem Konfigurieren der virtuellen Maschinen bei jeder virtuellen Maschine im VM-Set an, und installieren Sie SnapCenter-Server in beiden Knoten.
3. Erstellen Sie den Cluster in 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. Sehen Sie sich die Details zur Hochverfügbarkeit an.
   ```
   Get-SmServerConfig
   ```
6. Falls erforderlich, erstellen Sie den sekundären Host neu.
   ```
   Set-SmRepositoryConfig -RebuildSlave -Verbose
   ```
7. Failover auf den zweiten Host.
   ```
   Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
   ```

== Wechsel von NLB zu F5 für hohe Verfügbarkeit

Sie können Ihre SnapCenter HA-Konfiguration von Network Load Balancing (NLB) auf F5 Load Balancer ändern.

Schritte

1. Konfigurieren Sie SnapCenter-Server für hohe Verfügbarkeit mit F5. "Weitere Informationen ."
2. Starten Sie PowerShell auf dem Host des SnapCenter Servers.
3. Starten Sie eine Sitzung mit dem Cmdlet "Open-SmConnection", und geben Sie dann Ihre Anmeldeinformationen ein.
4. Aktualisieren Sie den SnapCenter-Server, um mit dem Cmdlet "Update-SmServerCluster" auf die F5-Cluster-IP-Adresse zu verweisen.

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

Hochverfügbarkeit für das SnapCenter MySQL Repository

MySQL-Replikation ist eine Funktion von MySQL Server, mit der Sie Daten von einem MySQL-Datenbankserver (Master) auf einen anderen MySQL-Datenbankserver (Slave) replizieren können. SnapCenter unterstützt die MySQL-Replikation für Hochverfügbarkeit nur auf zwei NLB-fähigen (Network Load Balancing-enabled) Knoten.

SnapCenter führt Lese- oder Schreibvorgänge im Master-Repository durch und leitet die Verbindung zum Slave-Repository weiter, wenn ein Fehler im Master-Repository auftritt. Das Slave-Repository wird dann zum Master-Repository. SnapCenter unterstützt außerdem die umgekehrte Replizierung, die nur während des Failover aktiviert ist.

Wenn Sie die MySQL High Availability (HA)-Funktion verwenden möchten, müssen Sie den Network Load Balancer (NLB) auf dem ersten Knoten konfigurieren. Das MySQL-Repository ist auf diesem Knoten als Teil der Installation installiert. Bei der Installation von SnapCenter auf dem zweiten Knoten müssen Sie sich mit F5 des ersten Knotens verbinden und auf dem zweiten Knoten eine Kopie des MySQL-Repository erstellen.

SnapCenter bietet die *get-SmRepositoryConfig* und *set-SmRepositoryConfig* PowerShell Commandlets zur Verwaltung der MySQL Replikation.

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

Beachten Sie die Einschränkungen für die MySQL HA-Funktion:

- NLB und MySQL HA werden nicht über zwei Knoten hinaus unterstützt.
- Ein Wechsel von einer eigenständigen SnapCenter-Installation zu einer NLB-Installation oder umgekehrt und das Umschalten von einer MySQL-Standalone-Konfiguration auf MySQL HA wird nicht unterstützt.
- Automatisches Failover wird nicht unterstützt, wenn die Slave-Repository-Daten nicht mit den Master-Repository-Daten synchronisiert werden.

  Sie können ein erzwungenes Failover initiieren, indem Sie das Cmdlet *set-SmoryConfig* verwenden.

- Wenn ein Failover initiiert wird, können Jobs, die ausgeführt werden, fehlschlagen.

  Wenn ein Failover aufgrund eines MySQL Servers oder SnapCenter Servers ausfällt, können alle ausgeführten Jobs fehlschlagen. Nach dem Failover zum zweiten Node 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 (Role Based Access Control, RBAC)

Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu

Um die rollenbasierte Zugriffssteuerung für SnapCenter-Benutzer zu konfigurieren, können Sie Benutzer oder Gruppen hinzufügen und Rollen zuweisen. Die Rolle legt die Optionen fest, auf die SnapCenter-Benutzer zugreifen können.

Bevor Sie beginnen

- Sie müssen sich als „SnapCenterAdmin“-Rolle angemeldet haben.
- Sie müssen die Benutzer- oder Gruppenkonten in Active Directory im Betriebssystem oder in der Datenbank erstellt haben. Sie können SnapCenter nicht zum Erstellen dieser Konten verwenden.

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

- SnapCenter umfasst mehrere vordefinierte Rollen.

  Sie können diese Rollen entweder dem Benutzer zuweisen oder neue Rollen erstellen.

- AD-Benutzer und AD-Gruppen, die SnapCenter RBAC hinzugefügt werden, müssen über DIE LESEBERECHTIGUNG auf dem Benutzer-Container und dem Computer-Container im Active Directory verfügen.
- Nachdem Sie einem Benutzer oder einer Gruppe eine Rolle zugewiesen haben, die die entsprechenden Berechtigungen enthält, müssen Sie den Benutzerzugriff auf SnapCenter-Ressourcen wie Hosts und Speicherverbindungen zuweisen.

  Auf diese Weise 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 RBAC-Berechtigungen und Effizienzfunktionen zu nutzen.
- Sie können Assets wie Host, Ressourcengruppen, Richtlinien, Storage-Verbindungen, Plug-in, Und Anmeldeinformationen für den Benutzer beim Erstellen des Benutzers oder der Gruppe.
- Die Mindestwerte, die Sie einem Benutzer zur Durchführung bestimmter Vorgänge zuweisen sollten, sind:

Betrieb	Zuweisung von Assets
Ressourcen schützen	Host, Richtlinie
Backup	Host, Ressourcengruppe und Richtlinie
Wiederherstellen	Host, Ressourcengruppe
Klonen	Host, Ressourcengruppe und Richtlinie
Lebenszyklus von Klonen	Host
Erstellen Sie eine Ressourcengruppe	Host

- Wenn ein neuer Knoten zu einem Windows Cluster oder einer DAG (Exchange Server Database Availability Group)-Ressource hinzugefügt wird und wenn dieser neue Knoten einem Benutzer zugewiesen ist, müssen Sie das Element dem Benutzer oder der Gruppe neu zuweisen, um den neuen Knoten dem Benutzer oder der Gruppe hinzuzufügen.

  Sie sollten den RBAC-Benutzer oder die Gruppe dem Cluster oder der DAG neu zuweisen, um den neuen Node auch dem RBAC-Benutzer oder der Gruppe einzuschließen. Sie verfügen beispielsweise über ein Cluster mit zwei Nodes und haben dem Cluster einen RBAC-Benutzer oder eine Gruppe zugewiesen. Wenn Sie dem Cluster einen weiteren Node hinzufügen, sollten Sie den RBAC-Benutzer oder die Gruppe dem Cluster neu zuweisen, um den neuen Node für den Benutzer oder die Gruppe der RBAC einzubeziehen.

- Wenn Sie planen, Snapshots zu replizieren, müssen Sie dem Benutzer, der den Vorgang durchführt, die Speicherverbindung für das Quell- und das Ziel-Volume zuweisen.

  Sie sollten Assets hinzufügen, bevor Sie den Benutzern Zugriff zuweisen.

Wenn Sie zum Schutz von VMs, VMDKs oder Datastores das SnapCenter Plug-in für VMware vSphere verwenden, sollten Sie ein vCenter Benutzer zu einem SnapCenter Plug-in für VMware vSphere hinzufügen. Informationen zu VMware vSphere-Rollen finden Sie unter "Vordefinierte Rollen in Paketen mit SnapCenter Plug-in für 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 Workgroup hinzufügen:

Für dieses Feld…	Tun Sie das…
Zugriffstyp	Wählen Sie entweder Domäne oder Arbeitsgruppe aus Für den Authentifizierungstyp Domäne müssen Sie den Domänennamen des Benutzers oder der Gruppe angeben, dem Sie den Benutzer zu einer Rolle hinzufügen möchten. Standardmäßig wird er mit dem angemeldeten Domänennamen ausgefüllt. Sie müssen die nicht vertrauenswürdige Domäne auf der Seite **Einstellungen** > **Globale Einstellungen** > **Domain-Einstellungen** registrieren.
Typ	Wählen Sie entweder Benutzer oder Gruppe aus SnapCenter unterstützt nur Sicherheitsgruppen, nicht die Vertriebsgruppe.
Benutzername	a. Geben Sie den teilweisen Benutzernamen ein, und klicken Sie dann auf **Hinzufügen**. Bei Benutzername wird die Groß-/Kleinschreibung berücksichtigt. b. Wählen Sie den Benutzernamen aus der Suchliste aus. Wenn Sie Benutzer aus einer anderen Domäne oder einer nicht vertrauenswürdigen Domäne hinzufügen, sollten Sie den Benutzernamen vollständig eingeben, da keine Suchliste für domänenübergreifende Benutzer vorhanden ist. Wiederholen Sie diesen Schritt, um der ausgewählten Rolle weitere Benutzer oder Gruppen hinzuzufügen.
Rollen	Wählen Sie die Rolle aus, der Sie den Benutzer hinzufügen möchten.

4. Klicken Sie auf **Zuweisen** und dann auf der Seite „Assets zuweisen“ auf:
   a. Wählen Sie den Typ des Assets aus der Dropdown-Liste **Asset** aus.
   b. Wählen Sie in der Asset-Tabelle das Asset aus.

      Die Assets werden nur aufgeführt, wenn der Benutzer die Assets zu SnapCenter hinzugefügt hat.

   c. Wiederholen Sie diesen Vorgang für alle erforderlichen Assets.
   d. Klicken Sie Auf **Speichern**.
5. Klicken Sie Auf **Absenden**.

   Nachdem Sie Benutzer oder Gruppen hinzugefügt und Rollen zugewiesen haben, aktualisieren Sie die Ressourcenliste.

Erstellen Sie eine Rolle

Zusätzlich zur Nutzung vorhandener SnapCenter-Rollen können Sie eigene Rollen erstellen und die Berechtigungen anpassen.

Sie sollten sich als „SnapCenterAdmin“-Rolle angemeldet haben.

Schritte

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

   ⓘ In Benutzernamen und Gruppennamen können nur die folgenden Sonderzeichen eingefügt werden: Leerzeichen ( ), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:).

5. Wählen Sie **Alle Mitglieder dieser Rolle können Objekte anderer Mitglieder** sehen, damit andere Mitglieder der Rolle nach der Aktualisierung der Ressourcenliste Ressourcen wie Volumes und Hosts sehen können.

   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 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 gewähren.
7. Klicken Sie Auf **Absenden**.

Fügen Sie mithilfe von Sicherheits-Login-Befehlen eine ONTAP RBAC-Rolle hinzu

Sie können mit den Sicherheits-Login-Befehlen eine ONTAP RBAC-Rolle hinzufügen,

wenn auf Ihren Storage-Systemen Clustered ONTAP ausgeführt wird.

Bevor Sie beginnen

- Bevor Sie eine ONTAP RBAC-Rolle für Storage-Systeme mit Clustered ONTAP erstellen, müssen Sie Folgendes angeben:
  - Die Aufgabe (oder Aufgaben), die Sie ausführen möchten
  - Die zum Ausführen dieser Aufgaben erforderlichen Berechtigungen
- Zum Konfigurieren einer RBAC-Rolle müssen Sie die folgenden Aktionen durchführen:
  - Gewähren Sie Berechtigungen für Befehle und/oder Befehlsverzeichnisse.

    Für jedes Befehlsverzeichnis gibt es zwei Zugriffsebenen: All-Access und Read-Only.

  Sie müssen immer zuerst die All-Access-Berechtigungen zuweisen.

  - Rollen Benutzern zuweisen.
  - Sie können Ihre Konfiguration abhängig davon, ob Ihre SnapCenter Plug-ins für das gesamte Cluster mit der Cluster Administrator-IP verbunden oder direkt mit einer SVM im Cluster verbunden sind.

Über diese Aufgabe

Um die Konfiguration dieser Rollen auf Storage-Systemen zu vereinfachen, können Sie das RBAC Benutzer Creator für Data ONTAP Tool verwenden, das im NetApp Communities Forum verfügbar ist.

Dieses Tool verarbeitet automatisch die korrekte Einrichtung der ONTAP-Berechtigungen. Beispielsweise fügt das Tool RBAC Benutzer Creator für Data ONTAP automatisch die Berechtigungen in der richtigen Reihenfolge ein, sodass zuerst die Berechtigungen für alle Zugriffe angezeigt werden. Wenn Sie zuerst die schreibgeschützten Berechtigungen hinzufügen und dann die All-Access-Berechtigungen hinzufügen, markiert ONTAP die All-Access-Berechtigungen als Duplikate und ignoriert sie.

Wenn Sie zu einem späteren Zeitpunkt ein Upgrade von SnapCenter oder ONTAP durchführen, sollten Sie das Tool RBAC User Creator für Data ONTAP erneut ausführen, um die zuvor erstellten Benutzerrollen zu aktualisieren. Benutzerrollen, die für eine frühere Version von SnapCenter oder ONTAP erstellt wurden, funktionieren nicht ordnungsgemäß mit aktualisierten Versionen. Wenn Sie das Tool erneut ausführen, übernimmt es automatisch die Aktualisierung. Sie müssen die Rollen nicht neu erstellen.

Weitere Informationen zum Einrichten von ONTAP RBAC-Rollen finden Sie unter "ONTAP 9 Administratorauthentifizierung und RBAC-Energiehandbuch".

Aus Konsistenzgründen bezieht sich die SnapCenter-Dokumentation auf die Rollen als Verwenden von Berechtigungen. Die OnCommand System Manager GUI verwendet den Begriff *attribut* anstelle von *Privilege*. Beim Einrichten von ONTAP RBAC-Rollen bedeuten beide Begriffe dasselbe.

Schritte

1. Erstellen Sie auf dem Storage-System 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, werden standardmäßig Cluster-Administratoren verwendet.
- Role_Name ist der Name, den Sie für die Rolle angeben.
- Befehl ist die ONTAP Funktion.

> Sie müssen diesen Befehl für jede Berechtigung wiederholen. Beachten Sie, dass vor schreibgeschützten Befehlen All-Access-Befehle aufgelistet 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 durch Eingabe des folgenden Befehls:

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

- User_Name ist der Name des von Ihnen erstellten Benutzers.
- <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.
- svm_Name ist der Name der SVM.

3. Weisen Sie dem Benutzer die Rolle durch Eingabe des folgenden Befehls zu:

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

- <user_Name> ist der Name des Benutzers, den Sie in Schritt 2 erstellt haben. Mit diesem Befehl können Sie den Benutzer so ändern, dass er der Rolle zugeordnet wird.
- <svm_Name> ist der Name der SVM.
- <Role_Name> ist der Name der Rolle, die Sie in Schritt 1 erstellt haben.
- <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.

4. Überprüfen Sie, ob der Benutzer ordnungsgemäß 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

Beim Erstellen einer Rolle für einen neuen SVM-Benutzer in ONTAP müssen Sie verschiedene ONTAP-CLI-Befehle ausführen. Diese Rolle ist erforderlich, wenn Sie SVMs in ONTAP für die Verwendung mit SnapCenter konfigurieren und Sie nicht die vsadmin-Rolle 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 die Rolle diesem Benutzer 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 verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

Ab 5.0 werden vServer Admin-Benutzer nur noch mit REST-APIs unterstützt. Wenn Sie Rollen erstellen möchten, die nicht vserver admin verwenden, sollten Sie ZAPI verwenden.

- `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 ONTAP-Cluster-Rollen mit minimalen Berechtigungen

Sie sollten eine ONTAP-Cluster-Rolle 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-Cluster-Rolle zu erstellen und minimale Berechtigungen 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 die Rolle diesem Benutzer zu.

```
security login create -user <user_name\> -vserver <cluster_name\> -application
ontapi -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 verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um Cluster-Rollen zu erstellen und Berechtigungen zuzuweisen.

Ab SnapCenter 5.0 werden Cluster-Admin-Benutzer nur über REST-APIs unterstützt. Wenn Sie Rollen erstellen möchten, die nicht Cluster Admin verwenden, sollten Sie ZAPI verwenden.

- `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 "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`

Konfigurieren Sie IIS-Anwendungspools, um die Leseberechtigungen von Active Directory zu aktivieren

Sie können IIS (Internet Information Services) auf Ihrem Windows-Server so konfigurieren, dass ein benutzerdefiniertes Application Pool-Konto erstellt wird, 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 in der Liste Anwendungspools SnapCenter aus, und klicken Sie dann im Bereich Aktionen 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 einen Domänenbenutzer oder Domänenadministratornamen mit der Berechtigung Active Directory Lesen ein.
6. Klicken Sie auf OK.

   Das benutzerdefinierte Konto ersetzt das integrierte ApplicationPoolIdentity-Konto für den SnapCenter-Anwendungspool.

Konfigurieren Sie die Einstellungen für das Prüfprotokoll

Für jede Aktivität des SnapCenter Servers werden Audit-Protokolle erstellt. Standardmäßig sind Audit-Protokolle am installierten Standardspeicherort gesichert *C:\Program Files\NetApp\SnapCenter WebApp\Audit*\.

Prüfprotokolle werden durch die Generierung von Digital Signed Digest für jedes einzelne Audit-Ereignis gesichert, um es vor nicht autorisierten Änderungen zu schützen. Die generierten Digest-Dateien werden in der separaten Prüfsumme-Prüfdatei aufbewahrt und werden regelmäßig Integritätsprüfungen unterzogen, um die Integrität des Inhalts zu gewährleisten.

Sie sollten sich als „SnapCenterAdmin“-Rolle angemeldet haben.

Über diese Aufgabe

- Warnmeldungen werden in den folgenden Szenarien gesendet:
  - Der Zeitplan für die Integritätsprüfung des Überwachungsprotokolls oder der Syslog-Server ist aktiviert oder deaktiviert
  - Prüfung der Integritätsprüfung der Protokolle, Audit-Protokoll oder Ausfall des Syslog-Serverprotokolls
  - Nur wenig Speicherplatz
- E-Mails werden nur gesendet, wenn die Integritätsprüfung fehlschlägt.
- Sie sollten sowohl das Verzeichnis des Prüfprotokolls als auch die Verzeichnispfade für das Prüfsumme-Protokoll gemeinsam ändern. Es ist nicht möglich, nur eine dieser Änderungen vorzunehmen.
- Wenn das Verzeichnis des Prüfprotokolls und die Verzeichnispfade der Prüfsumme geändert werden, kann die Integritätsprüfung nicht für die am früheren Speicherort vorhandenen Prüfprotokolle durchgeführt werden.
- Verzeichnis für Prüfsumme und Prüfsumme für Prüfprotokolle sollten sich auf dem lokalen Laufwerk des SnapCenter Servers befinden.

  Freigegebene oder netzwerkbasierte Laufwerke werden nicht unterstützt.

- Wenn das UDP-Protokoll in den Einstellungen des Syslog-Servers verwendet wird, sind Fehler aufgrund des Ports ausgefallen oder nicht verfügbar. Es kann weder als Fehler noch als Warnung in SnapCenter erfasst werden.
- Sie können Set-SmAuditSettings und Get-SmAuditSettings Befehle verwenden, um die Prüfprotokolle zu

konfigurieren.

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

Schritte

1. Navigieren Sie auf der Seite **Einstellungen** zu **Einstellungen** > **Globale Einstellungen** > **Prüfprotokoll-Einstellungen**.
2. Geben Sie im Abschnitt Prüfprotokoll die Details ein.
3. Geben Sie das Logverzeichnis **Audit** und das Verzeichnis **Prüfsumme-Prüfsumme-Protokoll** ein
   a. Geben Sie die maximale Dateigröße ein
   b. Geben Sie die maximale Anzahl von Protokolldateien ein
   c. Geben Sie den Prozentsatz der Speicherplatznutzung ein, um eine Meldung zu senden
4. (Optional) Aktivieren Sie **UTC-Uhrzeit protokollieren**.
5. (Optional) Aktivieren Sie **Auditprotokoll Integritätsprüfung Zeitplan** und klicken Sie auf **Integritätsprüfung starten**, um die Integritätsprüfung nach Bedarf zu prüfen.

   Sie können auch den Befehl **Start-SmAuditIntegritätCheck** ausführen, um die Integritätsprüfung bei Bedarf zu starten.

6. (Optional) Aktivieren Sie die Weiterleitung von Audit-Protokollen an Remote-Syslog-Server und geben Sie die Details des Syslog-Servers ein.

   Sie sollten das Zertifikat vom Syslog-Server in den 'Trusted Root' für das TLS 1.2-Protokoll importieren.

   a. Geben Sie Syslog Server Host Ein
   b. Geben Sie Den Syslog-Server-Port Ein
   c. Geben Sie Syslog Server Protocol Ein
   d. RFC-Format eingeben
7. Klicken Sie Auf **Speichern**.
8. Durch Klicken auf **Monitor** > **Jobs** können Sie die Integritätsprüfungen und die Überprüfung des Festplattenspeichers einsehen.

Storage-Systeme hinzufügen

Sie sollten das Storage-System einrichten, mit dem SnapCenter Zugriff auf ONTAP Storage oder Amazon FSX für NetApp ONTAP erhalten, um Datensicherungs- und Bereitstellungsvorgänge durchzuführen.

Sie können entweder eine eigenständige SVM oder ein Cluster aus mehreren SVMs hinzufügen. Wenn Sie Amazon FSX für NetApp ONTAP verwenden, können Sie entweder FSX Admin LIF aus mehreren SVMs mit fsxadmin-Konto hinzufügen oder FSX SVM in SnapCenter hinzufügen.

Bevor Sie beginnen

- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.

- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Über diese Aufgabe

- Wenn Sie Speichersysteme konfigurieren, können Sie auch die Funktionen für das Ereignismanagement (EMS) & AutoSupport aktivieren. Das AutoSupport Tool erfasst Daten zum Systemzustand des Systems und sendet die Daten automatisch an den technischen Support von NetApp. Damit können sie Fehler im System Ihres Systems beheben.

  Wenn Sie diese Funktionen aktivieren, sendet SnapCenter AutoSupport-Informationen an das Storage-System und EMS-Meldungen an das Syslog-System, wenn eine Ressource geschützt ist, eine Wiederherstellung oder ein Klonvorgang erfolgreich abgeschlossen wird oder ein Vorgang ausfällt.

- Wenn Sie planen, Snapshots auf ein SnapMirror Ziel oder ein SnapVault Ziel zu replizieren, müssen Sie Storage-Systemverbindungen für die Ziel-SVM oder das Cluster sowie die Quell-SVM oder das Cluster einrichten.

> ⓘ Wenn Sie das Kennwort des Speichersystems ändern, können geplante Jobs, Backup-Vorgänge bei Bedarf und Wiederherstellungsvorgänge fehlschlagen. Nach dem Ändern des Kennworts des Speichersystems können Sie das Passwort 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 Add Storage System die folgenden Informationen ein:

Für dieses Feld…	Tun Sie das…
Storage-System	Geben Sie den Namen des Storage-Systems oder die IP-Adresse ein. Die Namen des Speichersystems, ohne den Domänennamen zu enthalten, müssen 15 oder weniger Zeichen enthalten und die Namen müssen aufgelöst werden können. Um Verbindungen zu Speichersystemen mit Namen zu erstellen, die mehr als 15 Zeichen enthalten, können Sie das Cmdlet "Add-SmStorageConnectionPowerShell" verwenden. Bei Storage-Systemen mit MetroCluster-Konfiguration (MCC) wird sowohl lokale als auch Peer-Cluster registrieren, um unterbrechungsfreien Betrieb zu gewährleisten. SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss über einen eindeutigen Namen verfügen. Nachdem Sie die Storage-Verbindung zu SnapCenter hinzugefügt haben, sollten Sie die SVM oder den Cluster nicht mithilfe von ONTAP umbenennen. Wenn eine SVM mit einem kurzen Namen oder einem FQDN hinzugefügt wird, muss sie sowohl aus dem SnapCenter als auch dem Plug-in-Host resolable sein.
Benutzername/Passwort	Geben Sie die Anmeldedaten des Speicherbenutzers ein, der über die erforderlichen Berechtigungen für den Zugriff auf das Speichersystem verfügt.

Für dieses Feld…	Tun Sie das…
Einstellungen für Ereignismanagement-System (EMS) und AutoSupport	Wenn Sie EMS-Meldungen an das Syslog-Speichersystem senden möchten oder wenn Sie AutoSupport-Meldungen für den angewendeten Schutz, abgeschlossene Wiederherstellungsvorgänge oder fehlgeschlagene Vorgänge an das Speichersystem senden möchten, aktivieren Sie das entsprechende Kontrollkästchen. Wenn Sie das Kontrollkästchen **AutoSupport-Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem senden** aktivieren, ist das Kontrollkästchen * SnapCenter-Ereignisse in syslog* aktiviert, da EMS-Nachrichten zur Aktivierung von AutoSupport-Benachrichtigungen erforderlich sind.

4. Klicken Sie auf **Mehr Optionen**, wenn Sie die Standardwerte ändern möchten, die Plattform, Protokoll, Port und Timeout zugewiesen sind.

   a. Wählen Sie unter Plattform eine der Optionen aus der Dropdown-Liste aus.

      Wenn die SVM das sekundäre Storage-System in einer Backup-Beziehung ist, aktivieren Sie das Kontrollkästchen **sekundär**. Wenn die Option **Sekundär** ausgewählt ist, führt SnapCenter keine Lizenzprüfung sofort durch.

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

   a. Wählen Sie im Protokoll das Protokoll aus, das während der SVM- oder Cluster-Einrichtung, normalerweise HTTPS, konfiguriert wurde.
   b. Geben Sie den Port ein, den das Speichersystem akzeptiert.

      Der Standardport 443 funktioniert in der Regel.

   c. Geben Sie die Zeit in Sekunden ein, die verstreichen soll, bevor die Kommunikationsversuche angehalten werden.

      Der Standardwert ist 60 Sekunden.

   d. Wenn die SVM über mehrere Managementschnittstellen 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 **Absenden**.

Ergebnis

Führen Sie auf der Seite Storage Systems aus dem Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

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

  Falls Sie FSX SVMs hinzugefügt haben, finden Sie hier die FSX SVMs.

- 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 Cluster-Namen klicken, werden im Abschnitt Storage Virtual Machines alle SVMs, die Teil des Clusters sind, angezeigt.

  Wenn dem ONTAP Cluster über die ONTAP-Benutzeroberfläche eine neue SVM hinzugefügt wird, klicken Sie auf **Neu entdecken**, um die neu hinzugefügte SVM anzuzeigen.

Wenn Sie ein Upgrade der FAS- oder AFF-Speichersysteme auf All-SAN-Array (ASA) durchgeführt haben, müssen Sie die Speicherverbindung im SnapCenter-Server aktualisieren, damit der neue Speichertyp in SnapCenter berücksichtigt wird.

Nach Ihrer Beendigung

Ein Cluster-Administrator muss AutoSupport auf jedem Node des Storage-Systems aktivieren, um E-Mail-Benachrichtigungen von allen Storage-Systemen zu senden, auf die SnapCenter Zugriff hat, indem der folgende Befehl über die Befehlszeile des Storage-Systems ausgeführt wird:

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

Der SVM-Administrator hat keinen Zugriff auf AutoSupport.

Controller-basierte SnapCenter Standard-Lizenzen hinzufügen

Wenn Sie FAS, AFF oder All SAN Array (ASA) Storage Controller verwenden, ist eine Controller-basierte Lizenz für SnapCenter Standard erforderlich.

Die Controller-basierte Lizenz weist folgende Merkmale auf:

- SnapCenter Standard-Nutzungsberechtigung ist beim Kauf von Premium oder Flash Bundle enthalten (nicht im Basispaket).
- Unbegrenzte Storage-Nutzung
- Sie kann entweder über den ONTAP System Manager oder die Storage-Cluster-Befehlszeile direkt zum FAS, AFF oder ASA Storage Controller hinzugefügt werden

  Sie geben keine Lizenzinformationen in der SnapCenter GUI für die Controller-basierten SnapCenter Lizenzen ein.

- Gesperrt an die Seriennummer des Controllers

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 GUI verwenden, um festzustellen, ob eine SnapManager Suite Lizenz auf primären Storage-Systemen von FAS, AFF oder ASA installiert ist, und um zu ermitteln, für welche Storage-

Systeme möglicherweise Lizenzen der SnapManager Suite erforderlich sind. Lizenzen der SnapManager Suite gelten nur für FAS, AFF und ASA SVMs oder Cluster auf primären Storage-Systemen.

> Wenn Sie auf Ihrem Controller bereits eine Lizenz für die SnapManager Suite besitzen, wird die Controller-basierte SnapCenter Standard-Lizenzberechtigung automatisch bereitgestellt. Die Namen SnapManagerSuite Lizenz und SnapCenter Standard Controller-basierte Lizenz werden austauschbar verwendet, aber sie beziehen sich auf dieselbe Lizenz.

Schritte

1. Wählen Sie im linken Navigationsbereich **Storage Systems** aus.
2. Wählen Sie auf der Seite Storage Systems 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 Cluster-Namen 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 License“ wird der folgende Status angezeigt:

   -  Zeigt an, dass eine SnapManager Suite-Lizenz auf einem primären Speichersystem von FAS, AFF oder ASA installiert ist.
   -  Zeigt an, dass keine SnapManager Suite-Lizenz auf einem primären Speichersystem von FAS, AFF oder ASA installiert ist.
   - Nicht zutreffend bedeutet, dass eine SnapManager Suite-Lizenz nicht anwendbar ist, da sich der Storage Controller auf Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select oder sekundären Speicherplattformen befindet.

Schritt 2: Identifizieren Sie die auf dem Controller installierten Lizenzen

Mit der ONTAP-Befehlszeile können Sie alle auf dem Controller installierten Lizenzen anzeigen. Sie sollten Cluster-Administrator auf dem FAS-, AFF- oder ASA-System sein.

> Die Controller-basierte SnapCenter Standard-Lizenz wird auf dem Controller als SnapManagerSuite-Lizenz angezeigt.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim NetApp Controller ein.
2. Geben Sie den Befehl license show ein, und zeigen Sie anschließend die Ausgabe an, um zu ermitteln, 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: 1-81-0000000000000000000000000xx
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 -
```

Da hier beispielsweise die SnapManagerSuite Lizenz installiert ist, ist keine zusätzliche SnapCenter Lizenzmaßnahme erforderlich.

Schritt 3: Rufen Sie die Seriennummer des Controllers ab

Sie benötigen die Controller-Seriennummer zum Abrufen der Seriennummer Ihrer Controller-basierten Lizenz. Sie können die Seriennummer des Controllers über die ONTAP-Befehlszeile abrufen. Sie sollten Cluster-Administrator auf dem FAS-, AFF- oder ASA-System sein.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim Controller ein.
2. Geben Sie den Befehl „System show -instance“ ein, und überprüfen Sie die Ausgabe, um die Controller-Seriennummer 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: xxxxxxxxx
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: xxxxxxxxx
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: Rufen Sie die Seriennummer der Controller-basierten Lizenz ab

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

Bevor Sie beginnen

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

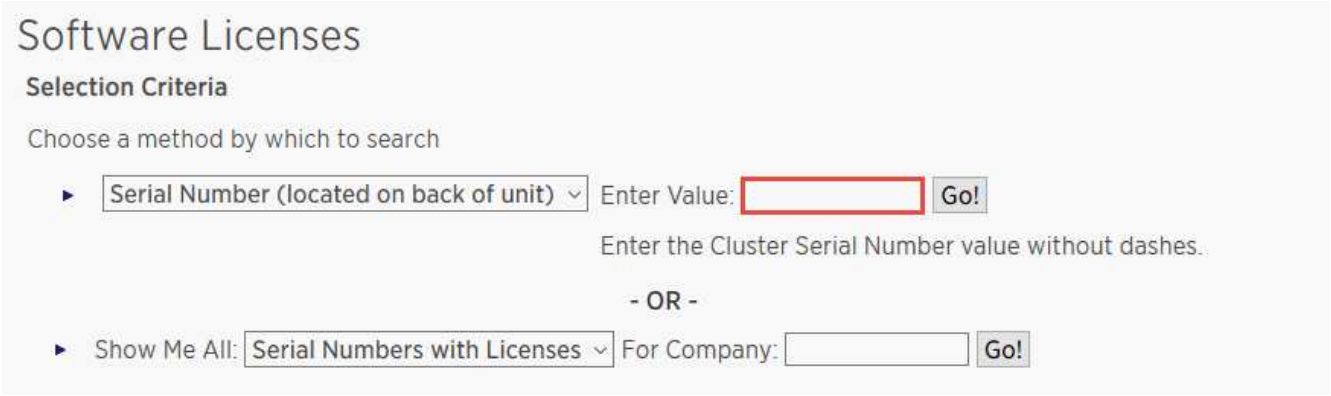
  Wenn Sie keine gültigen Anmeldedaten eingeben, werden keine Informationen für Ihre Suche

zurückgegeben.

- Sie sollten die Controller-Seriennummer angeben.

Schritte

1. Melden Sie sich beim an "NetApp Support-Website".
2. Navigieren Sie zu **Systems** > **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 **Go!**.



Eine Liste der Lizenzen für den angegebenen Controller wird angezeigt.

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

Schritt 5: Controller-basierte Lizenz hinzufügen

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

Bevor Sie beginnen

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

Über diese Aufgabe

Wenn Sie SnapCenter Testversionen mit FAS, AFF oder ASA Storage installieren möchten, erhalten Sie eine Evaluierungslizenz für das Premium Bundle, die auf Ihrem Controller installiert wird.

Wenn Sie SnapCenter auf Testbasis installieren möchten, sollten Sie sich an Ihren Ansprechpartner wenden, um eine Evaluierungslizenz für das Premium Bundle zu erhalten, die auf Ihrem Controller installiert wird.

Schritte

1. Loggen Sie sich über die ONTAP-Befehlszeile beim NetApp Cluster ein.
2. Fügen Sie den Lizenzschlüssel für die SnapManagerSuite hinzu:

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

Dieser Befehl ist auf der Administrator-Berechtigungsebene verfügbar.

3. Überprüfen Sie, ob 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 entfernen müssen (Seriennummer mit „50“ endet), 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 SnapCenter Standard-Lizenz verwenden.

Schritte

1. Öffnen Sie auf dem SnapCenter-Server ein PowerShell-Fenster, um das MySQL-Passwort zurückzusetzen.
   a. Führen Sie das Cmdlet "Open-SmConnection" aus, um eine Verbindungssitzung mit dem SnapCenter-Server für ein SnapCenterAdmin-Konto zu initiieren.
   b. Führen Sie das Set-RepositRepositRepositSmoryPassword aus, um das MySQL-Passwort zurückzusetzen.

      Informationen zu den Cmdlets finden Sie unter "SnapCenter Software Cmdlet Referenzhandbuch".

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

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

3. Entfernen Sie die Testlizenz aus der Datenbank:

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

Bereitstellung Ihres Storage-Systems

Bereitstellen von Storage auf Windows Hosts

Konfigurieren Sie LUN-Speicher

Mit SnapCenter können Sie eine FC-verbundene oder iSCSI-verbundene LUN konfigurieren. Sie können auch SnapCenter verwenden, um eine vorhandene LUN mit einem Windows-Host zu verbinden.

LUNs sind die grundlegende Storage-Einheit in einer SAN-Konfiguration. Der Windows-Host sieht LUNs auf Ihrem System als virtuelle Festplatten. Weitere Informationen finden Sie unter "ONTAP 9 SAN Configuration Guide".

Richten Sie eine iSCSI-Sitzung ein

Wenn Sie iSCSI zum Herstellen einer Verbindung zu einer LUN verwenden, müssen Sie eine iSCSI-Sitzung

starten, bevor Sie die LUN erstellen, um die Kommunikation zu ermöglichen.

Bevor Sie beginnen

- Sie müssen den Knoten des Speichersystems als iSCSI-Ziel definiert haben.
- Sie müssen den iSCSI-Dienst auf dem Speichersystem gestartet haben. "Weitere Informationen ."

Über diese Aufgabe

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

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

Wenn Sie den Namen eines iSCSI-Initiators ändern, ist der Zugriff auf iSCSI-Ziele beeinträchtigt. Nach Ändern des Namens müssen Sie eventuell die Ziele, auf die der Initiator Zugriff hat, neu konfigurieren, damit sie den neuen Namen erkennen können. Sie müssen sicherstellen, dass der Host nach Ändern des Namens eines iSCSI-Initiators neu gestartet wird.

Wenn Ihr Host über mehrere iSCSI-Schnittstellen verfügt, können Sie eine iSCSI-Sitzung mit einer IP-Adresse in der ersten Schnittstelle nicht von einer anderen Schnittstelle mit einer anderen IP-Adresse aus starten, wenn Sie eine iSCSI-Sitzung für SnapCenter eingerichtet haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite 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 Erstellen**.

   Der Assistent „Sitzung einrichten“ wird angezeigt.

6. Geben Sie im Assistenten zum Erstellen von Sitzungen das Ziel an:

In diesem Feld…	Eingeben…
Name des Ziel-Nodes	Der Knotenname des iSCSI-Ziels Wenn ein vorhandener Zielknotenname vorhanden ist, wird der Name im schreibgeschützten Format angezeigt.
Zielportaladresse	Die IP-Adresse des Zielnetzwerkportals
Zielportalport	Der TCP-Port des Zielnetzwerkportals
Adresse des Initiator-Portals	Die IP-Adresse des Initiator-Netzwerkportals

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

   SnapCenter richtet die iSCSI-Sitzung ein.

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

Trennen Sie eine iSCSI-Sitzung

Gelegentlich müssen Sie eine iSCSI-Sitzung von einem Ziel trennen, mit dem Sie mehrere Sitzungen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite 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. Wählen Sie aus der Liste der iSCSI-Sitzungen die Sitzung aus, die Sie trennen möchten, und klicken Sie auf **Sitzung trennen**.
6. Klicken Sie im Dialogfeld Sitzung trennen auf **OK**.

   SnapCenter trennt die iSCSI-Sitzung.

Erstellen und Verwalten von Initiatorgruppen

Sie erstellen Initiatorgruppen, um anzugeben, welche Hosts auf eine bestimmte LUN im Storage-System zugreifen können. Sie können SnapCenter eine Initiatorgruppe auf einem Windows Host erstellen, umbenennen, ändern oder löschen.

Erstellen einer Initiatorgruppe

Sie können SnapCenter zum Erstellen einer Initiatorgruppe auf einem Windows Host verwenden. Die Initiatorgruppe ist im Assistenten „Festplatte erstellen“ oder „Festplatte verbinden“ verfügbar, wenn Sie eine LUN zuordnen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **iGroup**.
3. Klicken Sie auf der Seite Initiatorgruppen auf **Neu**.
4. Definieren Sie im Dialogfeld Initiatorgruppe erstellen die Initiatorgruppe:

In diesem Feld…	Tun Sie das…
Storage-System	Wählen Sie die SVM für die LUN aus, die Sie der Initiatorgruppe zuordnen möchten.
Host	Wählen Sie den Host aus, auf dem Sie die Initiatorgruppe erstellen möchten.

In diesem Feld…	Tun Sie das…
Initiatorgruppe	Geben Sie den Namen der Initiatorgruppe ein.
Initiatoren	Wählen Sie den Initiator aus.
Typ	Wählen Sie den Initiatortyp, die iSCSI, FCP oder die Kombination aus (FCP und iSCSI) aus.

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

   SnapCenter erstellt die Initiatorgruppe auf dem Storage-System.

Benennen Sie eine Initiatorgruppe um

Sie können eine vorhandene Initiatorgruppe mit SnapCenter umbenennen.

Schritte

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

Ändern einer Initiatorgruppe

Sie können mit SnapCenter Initiatoren zu einer vorhandenen Initiatorgruppe hinzufügen. Beim Erstellen einer Initiatorgruppe können Sie nur einen Host hinzufügen. Wenn Sie eine Initiatorgruppe für ein Cluster erstellen möchten, können Sie die Initiatorgruppe ändern, um dieser Initiatorgruppe weitere Nodes hinzuzufügen.

Schritte

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

Löschen einer Initiatorgruppe

Sie können eine Initiatorgruppe mit SnapCenter löschen, wenn Sie sie nicht mehr benötigen.

Schritte

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

   SnapCenter löscht die Initiatorgruppe.

Erstellen und Verwalten von Festplatten

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

- SnapCenter unterstützt nur grundlegende Festplatten. Die dynamischen Festplatten werden nicht unterstützt.
- Für GPT ist nur eine Datenpartition und für MBR eine primäre Partition zulässig, die ein Volume mit NTFS oder CSVFS formatiert hat und einen Bereitstellungspfad hat.
- Unterstützte Partitionsstile: GPT, MBR; in einer VMware UEFI VM werden nur iSCSI-Laufwerke unterstützt

> SnapCenter unterstützt das Umbenennen einer Festplatte nicht. Wenn eine von SnapCenter gemanagte Festplatte umbenannt wird, ist der SnapCenter-Betrieb nicht erfolgreich.

Zeigen Sie die Festplatten auf einem Host an

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

Schritte

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

   Die Festplatten werden aufgelistet.

Anzeige geclusterter Festplatten

Sie können Cluster-Festplatten auf dem Cluster anzeigen, den Sie mit SnapCenter verwalten. Die Cluster-Laufwerke werden nur angezeigt, wenn Sie das Cluster aus dem Dropdown-Menü Hosts auswählen.

Schritte

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

   Die Festplatten werden aufgelistet.

Erstellen Sie mit FC verbundene oder mit iSCSI verbundene LUNs oder Festplatten

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

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

Bevor Sie beginnen

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

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

  Sie können auf einem mit SnapCenter erstellten Klon-Volume keine LUN erstellen, es sei denn, der Klon wurde bereits aufgeteilt.

- Sie müssen den FC- oder iSCSI-Service auf dem Storage-System gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem eingerichtet haben.
- Das SnapCenter-Plug-ins-Paket für Windows muss nur auf dem Host installiert sein, auf dem Sie den Datenträger 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 Failover Cluster gemeinsam genutzt.
- Wenn eine LUN von Hosts in einem Windows Server Failover Cluster freigegeben wird, die CSV (Cluster Shared Volumes) verwenden, müssen Sie die Festplatte auf dem Host erstellen, der die Cluster-Gruppe besitzt.

Schritte

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

   Der Assistent Datenträger erstellen wird geöffnet.

5. Geben Sie auf der Seite LUN-Name die LUN an:

In diesem Feld…	Tun Sie das…
Storage-System	Wählen Sie die SVM für die LUN aus.

In diesem Feld…	Tun Sie das…
LUN-Pfad	Klicken Sie auf **Durchsuchen**, um den vollständigen Pfad des Ordners auszuwählen, der die LUN enthält.
LUN-Name	Geben Sie den Namen der LUN ein.
Clustergröße	Wählen Sie die Block-Zuweisungsgröße der LUN für das Cluster aus. Die Cluster-Größe hängt vom Betriebssystem und den Applikationen ab.
LUN-Bezeichnung	Geben Sie optional einen beschreibenden Text für die LUN ein.

6. Wählen Sie auf der Seite Festplattentyp den Festplattentyp aus:

Auswählen…	Wenn…
Dedizierte Festplatte	Auf die LUN kann nur von einem Host zugegriffen werden. Ignorieren Sie das Feld **Ressourcengruppe**.
Freigegebenes Laufwerk	Die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt. Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld **Ressourcengruppe** ein. Sie müssen die Festplatte auf nur einem Host im Failover-Cluster erstellen.
Gemeinsam genutztes Cluster-Volume (CSV)	Die LUN wird von Hosts in einem Windows Server Failover Cluster, das CSV verwendet, gemeinsam verwendet. Geben Sie den Namen der Cluster-Ressourcengruppe in das Feld **Ressourcengruppe** ein. Stellen Sie sicher, dass der Host, auf dem Sie die Festplatte erstellen, der Besitzer der Cluster-Gruppe ist.

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

Eigenschaft	Beschreibung
Automatisches Zuweisen des Bereitstellungspunkts	SnapCenter weist auf der Grundlage des Systemlaufwerks automatisch einen Volume-Mount-Punkt zu. Beispiel: Wenn Ihr Systemlaufwerk C: Ist, erstellt Auto assign einen Mount-Punkt unter Ihrem Laufwerk C: (C:\scmnpt\). Die automatische Zuweisung wird für freigegebene Festplatten nicht unterstützt.
Weisen Sie einen Laufwerkbuchstaben zu	Befestigen Sie die Festplatte an dem Laufwerk, das Sie in der Dropdown-Liste neben ausgewählt haben.
Verwenden Sie den Volume-Bereitstellungspunkt	Befestigen Sie die Festplatte an dem im Feld nebenan angegebenen Laufwerkspfad. Das Root des Volume-Bereitstellungspunkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.
Weisen Sie keinen Laufwerksbuchstaben oder einen Volume-Bereitstellungspunkt zu	Wählen Sie diese Option, wenn Sie die Festplatte manuell in Windows mounten möchten.
Die LUN-Größe	Geben Sie die LUN-Größe an; Minimum 150 MB. Wählen Sie MB, GB oder TB in der angrenzenden Dropdown-Liste aus.
Verwenden Sie Thin Provisioning für das Volume, das diese LUN hostet	Thin Provisioning für die LUN Thin Provisioning weist nur so viel Speicherplatz zu, wie gleichzeitig benötigt wird. Dies ermöglicht es der LUN, die maximale verfügbare Kapazität effizient zu erweitern. Stellen Sie sicher, dass auf dem Volume genügend Speicherplatz verfügbar ist, um allen LUN-Storage, den Sie glauben, dass Sie benötigen werden, gerecht zu werden.

Eigenschaft	Beschreibung
Wählen Sie Partitionstyp	Wählen Sie GPT-Partition für eine GUID-Partitionstabelle oder MBR-Partition für einen Master Boot Record aus. MBR-Partitionen können falsche Ausrichtung in Windows Server Failover Clustern verursachen. Partitionsfestplatten der Unified Extensible Firmware Interface (UEFI) werden nicht unterstützt.

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

In diesem Feld…	Tun Sie das…
Host	Doppelklicken Sie auf den Cluster-Gruppennamen, um eine Dropdown-Liste anzuzeigen, in der die Hosts angezeigt werden, die zum Cluster gehören, und wählen Sie dann den Host für den Initiator aus. Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows-Server-Failover-Cluster gemeinsam genutzt wird.
Wählen Sie Host Initiator aus	Wählen Sie **Fibre Channel** oder **iSCSI** und wählen Sie dann den Initiator auf dem Host aus. Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit Multipath I/O (MPIO) verwenden.

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

Auswählen…	Wenn…
Erstellen einer neuen Initiatorgruppe für ausgewählte Initiatoren	Sie möchten eine neue Initiatorgruppe für die ausgewählten Initiatoren erstellen.
Wählen Sie eine vorhandene Initiatorgruppe aus, oder geben Sie eine neue Initiatorgruppe für ausgewählte Initiatoren an	Sie möchten eine vorhandene Initiatorgruppe für die ausgewählten Initiatoren angeben oder eine neue Initiatorgruppe mit dem angegebenen Namen erstellen. Geben Sie den Initiatorgruppennamen in das Feld * igroup Name* ein. Geben Sie die ersten Buchstaben des bestehenden Initiatorgruppennamens ein, um das Feld automatisch abzuschließen.

10. Überprüfen Sie auf der Zusammenfassungsseite Ihre Auswahl und klicken Sie dann auf **Fertig stellen**.

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

Ändern der Größe einer Festplatte

Sie können die Größe einer Festplatte bei sich ändernden Anforderungen Ihres Storage-Systems erhöhen oder reduzieren.

Über diese Aufgabe

- Bei einer LUN, die über Thin Provisioning bereitgestellt wurde, wird die Größe der ONTAP-lun-Geometrie als maximale Größe angezeigt.
- Bei LUNs mit Thick Provisioning 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 GPT-Partitionen haben eine Speichersystemgröße von maximal 16 TB.
- Es ist eine gute Idee, einen Snapshot vor der Größenänderung einer LUN zu erstellen.
- Wenn Sie eine LUN aus einem vor der Größe der LUN erstellten Snapshot wiederherstellen müssen, passt SnapCenter die LUN automatisch an die Größe des Snapshots an.

  Nach dem Restore müssen Daten, die der LUN nach der Größe der Größe hinzugefügt wurden, aus einem Snapshot wiederhergestellt werden, nachdem die Größe geändert wurde.

Schritte

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

   Die Festplatten werden aufgelistet.

4. Wählen Sie die Festplatte aus, die Sie ändern möchten, und klicken Sie dann auf **Größe**.
5. Verwenden Sie im Dialogfeld „Festplatte ändern“ das Schieberegler-Werkzeug, um die neue Größe der Festplatte 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 ist. Außerdem müssen Sie auf MB, GB oder TB klicken, um die Maßeinheit anzugeben.

6. Wenn Sie mit Ihren Einträgen zufrieden sind, klicken Sie ggf. auf **verkleinern** oder **erweitern**.

   SnapCenter Größe der Festplatte neu.

Schließen Sie eine Festplatte an

Sie können den Assistenten zum Verbinden von Festplatten verwenden, um eine vorhandene LUN mit einem Host zu verbinden, oder um eine getrennte LUN erneut zu verbinden.

Bevor Sie beginnen

- Sie müssen den FC- oder iSCSI-Service auf dem Storage-System gestartet haben.
- Wenn Sie iSCSI verwenden, müssen Sie eine iSCSI-Sitzung mit dem Speichersystem eingerichtet haben.
- Sie können eine LUN nicht mit mehr als einem Host verbinden, es sei denn, die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt.
- Wenn die LUN von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt wird, der CSV (Cluster Shared Volumes) verwendet, müssen Sie die Festplatte auf dem Host verbinden, der die Cluster-Gruppe besitzt.
- Das Plug-in für Windows muss nur auf dem Host installiert sein, auf dem Sie die Festplatte anschließen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Disks**.
3. Wählen Sie den Host aus der Dropdown-Liste **Host** aus.
4. Klicken Sie Auf **Verbinden**.

   Der Assistent zum Verbinden von Festplatten wird geöffnet.

5. Geben Sie auf der Seite LUN-Name die zu verbindende LUN an:

In diesem Feld…	Tun Sie das…
Storage-System	Wählen Sie die SVM für die LUN aus.
LUN-Pfad	Klicken Sie auf **Durchsuchen**, um den vollständigen Pfad des Volumes auszuwählen, das die LUN enthält.
LUN-Name	Geben Sie den Namen der LUN ein.
Clustergröße	Wählen Sie die Block-Zuweisungsgröße der LUN für das Cluster aus. Die Cluster-Größe hängt vom Betriebssystem und den Applikationen ab.
LUN-Bezeichnung	Geben Sie optional einen beschreibenden Text für die LUN ein.

6. Wählen Sie auf der Seite Festplattentyp den Festplattentyp aus:

Auswählen…	Wenn…
Dedizierte Festplatte	Auf die LUN kann nur von einem Host zugegriffen werden.

Auswählen…	Wenn…
Freigegebenes Laufwerk	Die LUN wird von Hosts in einem Windows Server Failover Cluster gemeinsam genutzt. Sie müssen die Festplatte nur mit einem Host im Failover-Cluster verbinden.
Gemeinsam genutztes Cluster-Volume (CSV)	Die LUN wird von Hosts in einem Windows Server Failover Cluster, das CSV verwendet, gemeinsam verwendet. Stellen Sie sicher, dass der Host, auf dem Sie eine Verbindung zur Festplatte herstellen, der Besitzer der Cluster-Gruppe ist.

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

Eigenschaft	Beschreibung
Automatische Zuweisung	Lassen Sie SnapCenter automatisch einen Volume Mount-Punkt basierend auf dem Systemlaufwerk zuweisen. Beispiel: Wenn Ihr Systemlaufwerk C: Ist, erstellt die Eigenschaft Auto assign einen Volume Mount Point unter Ihrem Laufwerk C: (C:\scmnpt\). Die Eigenschaft „Automatische Zuweisung“ wird für freigegebene Festplatten nicht unterstützt.
Weisen Sie einen Laufwerkbuchstaben zu	Legen Sie den Datenträger in die entsprechende Dropdown-Liste ein.
Verwenden Sie den Volume-Bereitstellungspunkt	Mounten Sie die Festplatte an den im Feld angrenzend angegebenen Laufwerkspfad. Das Root des Volume-Bereitstellungspunkts muss dem Host gehören, auf dem Sie die Festplatte erstellen.
Weisen Sie keinen Laufwerksbuchstaben oder einen Volume-Bereitstellungspunkt zu	Wählen Sie diese Option, wenn Sie die Festplatte manuell in Windows mounten möchten.

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

In diesem Feld…	Tun Sie das…
Host	Doppelklicken Sie auf den Cluster-Gruppennamen, um eine Dropdown-Liste anzuzeigen, in der die Hosts angezeigt werden, die zum Cluster gehören, und wählen Sie dann den Host für den Initiator aus. Dieses Feld wird nur angezeigt, wenn die LUN von Hosts in einem Windows-Server-Failover-Cluster gemeinsam genutzt wird.
Wählen Sie Host Initiator aus	Wählen Sie **Fibre Channel** oder **iSCSI** und wählen Sie dann den Initiator auf dem Host aus. Sie können mehrere FC-Initiatoren auswählen, wenn Sie FC mit MPIO verwenden.

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

Auswählen…	Wenn…
Erstellen einer neuen Initiatorgruppe für ausgewählte Initiatoren	Sie möchten eine neue Initiatorgruppe für die ausgewählten Initiatoren erstellen.
Wählen Sie eine vorhandene Initiatorgruppe aus, oder geben Sie eine neue Initiatorgruppe für ausgewählte Initiatoren an	Sie möchten eine vorhandene Initiatorgruppe für die ausgewählten Initiatoren angeben oder eine neue Initiatorgruppe mit dem angegebenen Namen erstellen. Geben Sie den Initiatorgruppennamen in das Feld * igroup Name* ein. Geben Sie die ersten Buchstaben des bestehenden Initiatorgruppennamens ein, um das Feld automatisch abzuschließen.

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 am Host.

Trennen Sie eine Festplatte

Sie können eine LUN ohne Auswirkungen auf den Inhalt der LUN von einem Host trennen, mit einer Ausnahme: Wenn Sie einen Klon vor dessen Trennung trennen, verlieren Sie den Inhalt des Klons.

Bevor Sie beginnen

- Stellen Sie sicher, dass die LUN nicht von einer Applikation verwendet wird.
- Stellen Sie sicher, dass die LUN nicht mit Monitoring-Software überwacht wird.
- Wenn die LUN gemeinsam genutzt wird, entfernen Sie die Abhängigkeiten der Cluster-Ressourcen aus der LUN, und überprüfen Sie, ob alle Nodes im Cluster eingeschaltet sind, ordnungsgemäß funktionieren und SnapCenter zur Verfügung stehen.

Über diese Aufgabe

Wenn Sie eine LUN in einem FlexClone Volume trennen, das SnapCenter erstellt hat, und keine anderen LUNs auf dem Volume sind verbunden, löscht SnapCenter das Volume. Vor dem Trennen der LUN zeigt SnapCenter eine Meldung an, dass das FlexClone Volume möglicherweise gelöscht wird.

Um das automatische Löschen des FlexClone Volume zu vermeiden, sollten Sie das Volume umbenennen, bevor Sie die letzte LUN trennen. Wenn Sie das Volume umbenennen, stellen Sie sicher, dass Sie mehrere Zeichen als nur das letzte Zeichen im Namen ändern.

Schritte

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

   Die Festplatten werden aufgelistet.
4. Wählen Sie das Laufwerk aus, das Sie trennen möchten, und klicken Sie dann auf **Trennen**.
5. Klicken Sie im Dialogfeld Disconnect Disk auf **OK**.

   SnapCenter trennt die Verbindung der Festplatte.

Löschen Sie eine Festplatte

Sie können einen Datenträger löschen, wenn Sie ihn nicht mehr benötigen. Nach dem Löschen eines Datenträgers können Sie das Löschen nicht rückgängig machen.

Schritte

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

   Die Festplatten werden aufgelistet.
4. Wählen Sie den Datenträger aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie im Dialogfeld Datenträger löschen auf **OK**.

   SnapCenter löscht die Festplatte.

SMB-Freigaben erstellen und managen

Um eine SMB3-Freigabe auf einer Storage Virtual Machine (SVM) zu konfigurieren, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell Commandlets verwenden.

Best Practice: die Verwendung der Cmdlets wird empfohlen, da es Ihnen ermöglicht, die Vorteile von Vorlagen mit SnapCenter zur Automatisierung der Share-Konfiguration zu nutzen.

Die Vorlagen kapseln die Best Practices für die Volume- und Share-Konfiguration. Die Vorlagen finden Sie im Ordner Vorlagen im Installationsordner für das SnapCenter-Plug-ins-Paket für Windows.

Wenn Sie sich damit wohlfühlen, können Sie Ihre eigenen Vorlagen nach den bereitgestellten Modellen erstellen. Sie sollten die Parameter in der Cmdlet-Dokumentation überprüfen, bevor Sie eine benutzerdefinierte Vorlage erstellen.

Erstellen Sie eine SMB-Freigabe

Auf der Seite „SnapCenter Shares“ können Sie eine SMB3-Freigabe auf einer Storage Virtual Machine (SVM) erstellen.

Datenbanken auf SMB-Freigaben können nicht mit SnapCenter gesichert werden. SMB-Support ist auf die reine Provisionierung beschränkt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **Shares**.
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 Feld…	Tun Sie das…
Beschreibung	Geben Sie einen beschreibenden Text für die Freigabe ein.
Freigabename	Geben Sie den Freigabenamen ein, z. B. „Test_share“. Der Name, den Sie für die Freigabe eingeben, wird auch als Volume-Name verwendet. Der Share-Name: • Muss eine UTF-8-Zeichenfolge sein. • Die folgenden Zeichen dürfen nicht enthalten sein: Steuerzeichen von 0x00 bis 0x1F (beide inklusiv), 0x22 (doppelte Anführungszeichen) und die Sonderzeichen `\ / [ ] : (vertical bar) < > + = ; , ?`
Freigabepfad	• Klicken Sie in das Feld, um einen neuen Dateisystempfad einzugeben, z. B. /. • Doppelklicken Sie in das Feld, um eine Liste der vorhandenen Dateisystempfade auszuwählen.

6. Wenn Sie mit Ihren Einträgen 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 Host-Seite auf **Shares**.
3. Klicken Sie auf der Seite Freigaben im Feld **Storage Virtual Machine** auf, 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 von der SVM.

Rückgewinnung von Speicherplatz im Storage-System

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

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

Bevor Sie beginnen

- Sie müssen sicherstellen, dass der Prozess zur Rückgewinnung von Speicherplatz abgeschlossen wurde, bevor Sie eine Wiederherstellung durchführen.
- Wenn die LUN von Hosts in einem Windows-Server-Failover-Cluster gemeinsam genutzt wird, müssen Sie Speicherplatz auf dem Host, der die Cluster-Gruppe besitzt, freigeben.
- Um eine optimale Storage-Performance zu erzielen, sollten Sie so oft wie möglich eine Platzreklamation durchführen.

  Stellen Sie sicher, dass das gesamte NTFS-Dateisystem gescannt wurde.

Über diese Aufgabe

- Die Rückgewinnung von Speicherplatz ist zeitaufwändig und CPU-intensiv. Daher ist es normalerweise am besten, wenn die Auslastung des Storage-Systems und des Windows-Hosts niedrig ist.
- Die Speicherplatzrückgewinnung beansprucht fast allen verfügbaren Speicherplatz, nicht aber 100 Prozent.

- Sie sollten die Festplattendefragmentierung nicht gleichzeitig ausführen, da Sie Speicherplatz einsparen.

  Dadurch kann der Rückgewinnungsprozess verlangsamt werden.

Schritt

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

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

Drive_Path ist der der der LUN zugeordnete Laufwerkpfad.

Stellen Sie Storage mit PowerShell cmdlets bereit

Wenn Sie die SnapCenter GUI nicht zum Ausführen von Aufgaben zur Host-Bereitstellung und zur Speicherplatzrückgewinnung verwenden möchten, können Sie die PowerShell Commandlets verwenden, die vom SnapCenter Plug-in für Microsoft Windows zur Verfügung gestellt werden. Sie können Cmdlets direkt verwenden oder zu Skripten hinzufügen.

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

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

Wenn SnapCenter PowerShell-Cmdlets aufgrund des Entfernens von SnapDrive für Windows vom Server unterbrochen werden, lesen Sie "SnapCenter cmdlets defekt, wenn SnapDrive für Windows deinstalliert wird".

Bereitstellung von Storage 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 Cluster-Konfigurationen

  Unterstützung von maximal 16 Knoten auf VMware bei Verwendung des Microsoft iSCSI Software-Initiators oder bis zu zwei Knoten mit FC

- RDM-LUNs

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

  Unterstützt VMware Paravirtuellen SCSI-Controller 256 Festplatten können auf RDM-Festplatten unterstützt werden.

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Serverbezogene Einschränkungen bei VMware ESXi

- Das Installieren des Plug-ins für Windows auf einem Microsoft-Cluster auf virtuellen Maschinen mit ESXi-Anmeldedaten wird nicht unterstützt.

  Sie sollten Ihre vCenter-Anmeldedaten verwenden, wenn Sie das Plug-in für Windows auf geclusterten virtuellen Maschinen installieren.

- Alle Cluster-Knoten müssen dieselbe Ziel-ID (auf dem virtuellen SCSI-Adapter) für dieselbe geclusterte Festplatte verwenden.
- Wenn Sie eine RDM-LUN außerhalb des Plug-in für Windows erstellen, müssen Sie den Plug-in-Service neu starten, damit die neu erstellte Festplatte erkannt werden kann.
- Auf einem VMware Gastbetriebssystem können Sie keine iSCSI- und FC-Initiatoren gleichzeitig verwenden.

Minimale vCenter-Berechtigungen, die für SnapCenter RDM-Vorgänge erforderlich sind

Sie sollten die folgenden vCenter-Rechte auf dem Host haben, um RDM-Vorgänge in einem Gastbetriebssystem durchzuführen:

- Datastore: Datei Entfernen
- Host: Konfiguration > Speicherpartition Konfiguration
- Virtual Machine: Konfiguration

Sie müssen diese Berechtigungen einer Rolle auf 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 Sie 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 gemeinsame RDM Quorum und den gemeinsam genutzten Speicher außerhalb des Plug-ins erstellen und dann die Festplatten den virtuellen Maschinen im Cluster hinzufügen.

Ab ESXi 5.5 können Sie auch ESX iSCSI und FCoE Hardware verwenden, um einen Microsoft-Cluster zu managen. Das Plug-in für Windows bietet Out-of-Box-Unterstützung für Microsoft Cluster.

Anforderungen

Das Plug-in für Windows unterstützt Microsoft Cluster mithilfe von FC RDM LUNs auf zwei verschiedenen Virtual Machines, die zu zwei verschiedenen ESX- oder ESXi-Servern gehören, auch „Cluster Across“ genannt, wenn Sie die spezifischen Konfigurationsanforderungen erfüllen.

- Die Virtual Machines (VMs) müssen dieselbe Windows Serverversion ausführen.
- ESX oder ESXi Serverversionen müssen für jeden übergeordneten VMware Host die gleichen sein.
- Jeder übergeordnete Host muss mindestens zwei Netzwerkadapter haben.
- Es muss mindestens ein VMware Virtual Machine File System (VMFS) Datastore vorhanden sein, der von den beiden ESX- oder ESXi-Servern gemeinsam genutzt wird.

- VMware empfiehlt, den gemeinsam genutzten Datenspeicher auf einem FC SAN zu erstellen.

  Bei Bedarf kann auch der gemeinsam genutzte Datenspeicher über iSCSI erstellt werden.

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

  Sie können virtuelle Laufwerke nicht für gemeinsamen Speicher verwenden.

- Ein SCSI-Controller muss für jede Virtual Machine im Cluster im physischen Kompatibilitätsmodus konfiguriert sein:

  Für Windows Server 2008 R2 müssen Sie den LSI Logic SAS SCSI-Controller auf jeder virtuellen Maschine konfigurieren. Freigegebene LUNs können den vorhandenen LSI Logic SAS-Controller nicht verwenden, wenn nur einer seiner Typen vorhanden ist und dieser bereits mit dem Laufwerk C: Verbunden ist.

  SCSI-Controller vom Typ paravirtuell werden auf VMware Microsoft Clustern nicht unterstützt.

  > Wenn Sie einer gemeinsam genutzten LUN auf einer virtuellen Maschine im physischen Kompatibilitätsmodus einen SCSI-Controller hinzufügen, müssen Sie im VMware Infrastructure Client die Option **Raw Device Mapping** (RDM) und nicht die Option **Create a New Disk** auswählen.

- Die Cluster der Microsoft Virtual Machine 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 Initiatorgruppe mit Initiatoren aus mehreren Hosts erstellen.

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

- Stellen Sie sicher, dass Sie eine RDM LUN unter ESXi 5.0 mit einem FC-Initiator erstellen.

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

Einschränkungen

Das Windows-Plug-in unterstützt Microsoft Cluster mit FC/iSCSI RDM LUNs auf verschiedenen Virtual Machines, 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 Cluster-Umgebung.

  Der Initiator muss entweder FC oder Microsoft iSCSI sein, aber nicht beides.

- ESX iSCSI-Initiatoren und HBAs werden von freigegebenen Laufwerken in einem Microsoft-Cluster nicht unterstützt.

- Das Plug-in für Windows unterstützt keine Migration von Virtual Machines mit vMotion, wenn die Virtual Machine Teil eines Microsoft Clusters ist.
- Das Plug-in für Windows unterstützt MPIO nicht auf virtuellen Maschinen in einem Microsoft-Cluster.

Erstellen Sie eine gemeinsame FC RDM LUN

Bevor Sie in einem Microsoft Cluster Speicher zwischen den Knoten mit FC RDM LUNs teilen können, müssen Sie zuerst die gemeinsame Quorum-Festplatte und die freigegebene Speicherplatte erstellen und diese dann beiden virtuellen Maschinen im Cluster hinzufügen.

Das freigegebene Laufwerk wird mit dem Plug-in für Windows nicht erstellt. Sie sollten die gemeinsame LUN erstellen und dann jeder virtuellen Maschine im Cluster hinzufügen. Weitere Informationen finden Sie unter "Clustern Von Virtual Machines Über Physische Hosts Hinweg".

Konfigurieren Sie gesicherte MySQL-Verbindungen mit SnapCenter-Server

Sie können SSL-Zertifikate (Secure Sockets Layer) und Schlüsseldateien generieren, wenn Sie die Kommunikation zwischen SnapCenter Server und MySQL Server in Standalone-Konfigurationen oder NLB-Konfigurationen (Network Load Balancing) sichern möchten.

Konfigurieren Sie gesicherte MySQL-Verbindungen für eigenständige SnapCenter-Server-Konfigurationen

Sie können SSL-Zertifikate (Secure Sockets Layer) 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 im SnapCenter-Server konfigurieren.

Folgende Zertifikate werden generiert:

- CA-Zertifikat
- Öffentliches Serverzertifikat und private Schlüsseldatei
- Öffentliches Zertifikat des Clients und Datei des privaten Schlüssels

Schritte

1. Richten Sie die SSL-Zertifikate und Schlüsseldateien für MySQL-Server und -Clients unter Windows mithilfe des openssl-Befehls ein.

   Weitere Informationen finden Sie unter "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und -Schlüsseln mit openssl"

   > Der allgemeine Namenswert, der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendet wird, muss sich von dem allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen das Zertifikat und die Schlüsseldateien bei Servern fehl, die mit OpenSSL kompiliert werden.

Best Practice: der Server Fully Qualified Domain Name (FQDN) sollte als allgemeiner Name für das Serverzertifikat verwendet werden.

2. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den Ordner MySQL Data.

   Der Standardpfad des MySQL-Datenordners ist `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Aktualisieren Sie das CA-Zertifikat, das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, den privaten Serverschlüssel und die Pfade des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

   Die Standardkonfigurationsdatei für den MySQL-Server (my.ini) ist `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   Sie müssen das CA-Zertifikat, das öffentliche Serverzertifikat und die privaten Server-Schlüsselpfade im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

   Sie müssen im Abschnitt [Client] der MySQL-Serverkonfigurationsdatei (my.ini) das CA-Zertifikat, das öffentliche Clientzertifikat und die privaten Schlüsselpfade des Clients 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. Beenden Sie die Webanwendung des SnapCenter-Servers im Internetinformationsserver (IIS).
5. Starten Sie den MySQL-Dienst neu.
6. Aktualisieren Sie den Wert des Schlüssels MySQLProtocol in der Datei SnapManager.Web.UI.dll.config.

   Das folgende Beispiel zeigt den Wert des Schlüssels MySQLProtocol, der in der Datei SnapManager.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 bereitgestellt 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 Webanwendung des SnapCenter-Servers im IIS.

Konfigurieren Sie gesicherte MySQL-Verbindungen für HA-Konfigurationen

Sie können SSL-Zertifikate (Secure Sockets Layer) und Schlüsseldateien sowohl für die HA-Knoten (High Availability) 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-Nodes wird ein CA-Zertifikat generiert, und dieses CA-Zertifikat wird auf den anderen HA-Node kopiert.

- Öffentliche Zertifikate des Servers und private Schlüsseldateien des Servers für beide HA-Nodes
- Öffentliche Client-Zertifikate und private Schlüsseldateien von Clients für beide HA-Nodes

Schritte

1. Richten Sie beim ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL Server und Clients unter Windows mithilfe des openssl-Befehls ein.

Weitere Informationen finden Sie unter "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und -Schlüsseln mit openssl"

> Der allgemeine Namenswert, der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendet wird, muss sich von dem allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen das Zertifikat und die Schlüsseldateien bei Servern fehl, die mit OpenSSL kompiliert werden.

Best Practice: der Server Fully Qualified Domain Name (FQDN) sollte als allgemeiner Name für das Serverzertifikat verwendet werden.

2. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den Ordner MySQL Data.

   Der standardmäßige Ordner MySQL Data ist C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Aktualisieren Sie das CA-Zertifikat, das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, den privaten Serverschlüssel und die Pfade des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

   Die standardmäßige MySQL Server-Konfigurationsdatei (my.ini) lautet C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.in

   > Sie müssen im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) CA-Zertifikat, öffentliches Serverzertifikat und private Server-Schlüsselpfade angeben.

   Sie müssen im Abschnitt [Client] der MySQL-Server-Konfigurationsdatei (my.ini) im Abschnitt [Client] CA-Zertifikat, öffentliches Clientzertifikat und private Schlüsselpfade des Clients angeben.

   Im folgenden Beispiel werden die Zertifikate und Schlüsseldateien im Abschnitt [mysqld] der Datei my.ini im Standardordner C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data kopiert.

   ```
   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 öffentliche Serverzertifikate, private Serverschlüsseldateien, öffentliche Clientzertifikate und private Clientschlüsseldateien. Führen Sie die folgenden Schritte aus:

   a. Kopieren Sie das auf dem ersten HA-Knoten generierte CA-Zertifikat in den Ordner MySQL Data des zweiten NLB-Knotens.

      Der standardmäßige Ordner MySQL Data ist C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

      > Sie dürfen kein CA-Zertifikat erneut erstellen. Sie sollten nur das öffentliche Serverzertifikat, das öffentliche Zertifikat des Clients, die Datei des privaten Schlüssels und die Datei des privaten Clientschlüssels erstellen.

   b. Richten Sie beim ersten HA-Knoten die SSL-Zertifikate und Schlüsseldateien für MySQL Server und Clients unter Windows mithilfe des openssl-Befehls ein.

      "MySQL Version 5.7: Erstellen von SSL-Zertifikaten und -Schlüsseln mit openssl"

      > Der allgemeine Namenswert, der für das Serverzertifikat, das Clientzertifikat und die Schlüsseldateien verwendet wird, muss sich von dem allgemeinen Namenswert unterscheiden, der für das CA-Zertifikat verwendet wird. Wenn die allgemeinen Namenswerte identisch sind, schlagen das Zertifikat und die Schlüsseldateien bei Servern fehl, die mit OpenSSL kompiliert werden.

      Es wird empfohlen, den Server-FQDN als gemeinsamen Namen für das Serverzertifikat zu verwenden.

   c. Kopieren Sie die SSL-Zertifikate und Schlüsseldateien in den Ordner MySQL Data.

   d. Aktualisieren Sie das CA-Zertifikat, das öffentliche Serverzertifikat, das öffentliche Clientzertifikat, den privaten Serverschlüssel und die Pfade des privaten Clientschlüssels in der MySQL-Serverkonfigurationsdatei (my.ini).

      > Sie müssen das CA-Zertifikat, das öffentliche Serverzertifikat und die privaten Server-Schlüsselpfade im Abschnitt [mysqld] der MySQL-Serverkonfigurationsdatei (my.ini) angeben.

      Sie müssen im Abschnitt [Client] der MySQL-Serverkonfigurationsdatei (my.ini) das CA-Zertifikat, das öffentliche Clientzertifikat und die privaten Schlüsselpfade des Clients angeben.

      Im folgenden Beispiel werden die Zertifikate und Schlüsseldateien im Abschnitt [mysqld] der Datei my.ini im Standardordner C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data kopiert.

```
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. Beenden Sie die Webanwendung des SnapCenter-Servers im Internet Information Server (IIS) auf beiden HA-Knoten.
6. Starten Sie den MySQL Service auf beiden HA-Nodes neu.
7. Aktualisieren Sie den Wert des Schlüssels MySQLProtocol in der Datei SnapManager.Web.UI.dll.config für beide HA-Knoten.

   Das folgende Beispiel zeigt den Wert des Schlüssels MySQLProtocol, 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-Nodes 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 Webanwendung des SnapCenter Servers im IIS auf beiden HA-Knoten.
10. Verwenden Sie das Cmdlet Set-SmRepositoryConfig -RebuildSlave -Force PowerShell mit der Option -Force auf einem der HA-Knoten, um eine gesicherte MySQL-Replikation auf beiden HA-Knoten einzurichten.

    Selbst wenn der Replikationsstatus ordnungsgemäß ist, können Sie mit der Option -Force das Slave-Repository wiederherstellen.

Während der Installation auf Ihrem Windows-Host aktivierte Funktionen

Das SnapCenter-Serverinstallationsprogramm aktiviert die Windows-Funktionen und -Rollen auf Ihrem Windows-Host während der Installation. Diese sind möglicherweise für die Fehlerbehebung und die Wartung des Host-Systems interessant.

Kategorie	Funktion
Web-Server	• Internet Information Services • World Wide Web Services • Allgemeine HTTP-Funktionen ◦ Standarddokument ◦ Verzeichnisbrowsing ◦ HTTP-Fehler ◦ HTTP-Umleitung ◦ Statischer Inhalt ◦ WebDAV-Publishing • Systemzustand und Diagnose ◦ Benutzerdefinierte Protokollierung ◦ HTTP-Protokollierung ◦ Protokollierungs-Tools ◦ Monitor Anfordern ◦ Nachzeichnen • Performance-Funktionen ◦ Statische Inhaltskomprimierung • Sicherheit ◦ IP Sicherheit ◦ Grundlegende Authentifizierung ◦ Zentralisierte Unterstützung von SSL-Zertifikaten ◦ Authentifizierung Für Die Clientzertifikatzuordnung ◦ Authentifizierung für die IIS-Clientzertifikatzuordnung ◦ IP- und Domänenbeschränkungen ◦ Anforderungsfilterung ◦ URL-Autorisierung ◦ Windows Authentifizierung • Funktionen Zur Applikationsentwicklung ◦ .NET Extensibility 4.5 ◦ Initialisierung Der Applikation ◦ ASP.NET Core Hosting Bundle ab Version 8.0.5 mit allen nachfolgenden .NET 8 Patches ◦ Server-Seitige Umfasst ◦ WebSocket-Protokoll Management Tools IIS-Verwaltungskonsole

Kategorie	Funktion
IIS-Verwaltungsskripte und -Tools	• IIS-Verwaltungsdienst • Web-Management-Tools
.NET Framework 8.0.5 Features	• .NET Framework ab Version 8.0.5 und einschließlich aller nachfolgenden .NET 8-Patches • ASP.NET ab Version 8.0.5 und einschließlich aller nachfolgenden .NET 8-Patches • Windows Communication Foundation (WCF) HTTP Activation45 ◦ TCP-Aktivierung ◦ HTTP-Aktivierung Für . NETZSPEZIFISCHE Informationen zur Fehlerbehebung, siehe "SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl".
Message Queuing	• Message Queuing Services Stellen Sie sicher, dass keine anderen Anwendungen den MSMQ-Dienst verwenden, den SnapCenter erstellt und verwaltet. • RabbitMQ
Windows-Prozess-Aktivierungsdienst	• Prozessmodell
Konfigurations-APIs	Alle

Funktionen, die während der Installation auf dem Linux-Host aktiviert wurden

Der SnapCenter-Server installiert die unten aufgeführten Softwarepakete. Diese können für die Fehlerbehebung und die Wartung des Host-Systems interessant sein.

- Rabbitmq
- Nginx
- Erlang
- .NET Framework ab Version 8.0.5 und einschließlich aller nachfolgenden .NET 8-Patches
- PAM-Entwicklung
- PowerShell

Microsoft SQL Server Datenbanken schützen

SnapCenter Plug-in für Microsoft SQL Server

SnapCenter Plug-in für Microsoft SQL Server – Übersicht

Das SnapCenter Plug-in für Microsoft SQL Server ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das Management der applikationsgerechten Datensicherung von Microsoft SQL Server Datenbanken ermöglicht. Das Plug-in für SQL Server automatisiert Backups, Verifizierungen, Restores und Klonvorgänge in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für SQL Server installiert ist, können Sie mithilfe von SnapCenter mit NetApp SnapMirror Technologie gespiegelte Kopien von Backups auf einem anderen Volume erstellen. In Verbindung mit der NetApp SnapVault Technologie können Sie eine Disk-to-Disk-Backup-Replizierung zwecks Standard-Compliance oder Archivierung durchführen.

Welche Möglichkeiten bietet das SnapCenter Plug-in für Microsoft SQL Server

Wenn das SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung installiert ist, können Sie mit SnapCenter die SQL Server Datenbanken sichern, wiederherstellen und klonen.

Sie können die folgenden Aufgaben durchführen, die Backup-Vorgänge, Restore-Vorgänge 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 Protokoll-Backups für Modell-System-Datenbank erstellen.

- Stellen Sie Datenbankressourcen wieder her
  - Sie können Stammsystemdatenbanken, msdb-Systemdatenbanken wiederherstellen und Systemdatenbanken modellieren.
  - Sie können nicht mehrere Datenbanken, Instanzen und Verfügbarkeitsgruppen wiederherstellen.
  - Sie können die Systemdatenbank nicht in einem anderen Pfad wiederherstellen.
- Erstellung zeitpunktgenauer Klone von Produktionsdatenbanken

  Sie können keine Backup-, Wiederherstellungs-, Klon- und Klonvorgänge auf tempdb-Systemdatenbanken durchführen.

- Umgehende Überprüfung der Backup-Vorgänge oder Vermeidung von Verifizierungen bis zu einem späteren Zeitpunkt

  Die Überprüfung der SQL Server Systemdatenbank wird nicht unterstützt. SnapCenter klont die Datenbanken, um einen Verifizierungsvorgang durchzuführen. SnapCenter kann SQL Server Systemdatenbanken nicht klonen. Daher wird die Überprüfung dieser Datenbanken nicht unterstützt.

- Planen von Backup-Vorgängen und Klonvorgängen

- Überwachung von Backup-Vorgängen, Restore-Vorgängen und Klonvorgängen

> Das Plug-in für SQL Server unterstützt kein Backup und Recovery 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 NetApp Snapshot Technologie auf dem Storage-System integrieren. Um mit dem Plug-in für SQL Server zu arbeiten, verwenden Sie die Schnittstelle SnapCenter.

Das Plug-in für SQL Server umfasst folgende Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche powered by SnapCenter**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die Schnittstelle von SnapCenter ermöglicht die vollständige konsistente Backup- und Restore-Prozesse über Plug-ins hinweg, die zentrale Berichterstellung, die auf einen Blick basierende Dashboard-Ansichten verwenden, die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) einrichten und Jobs in allen Plug-ins überwachen. SnapCenter bietet außerdem eine zentralisierte Planung und ein Richtlinienmanagement zur Unterstützung von Backup- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

  Sie können routinemäßige SQL Server Backups planen, eine richtlinienbasierte Backup-Aufbewahrung konfigurieren und zeitpunktgenaue und minutengenaue Restore-Vorgänge einrichten. Zudem lässt sich die SQL Server Umgebung proaktiv überwachen, indem SnapCenter zum Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Unterbrechungsfreie NetApp Snapshots**

  Das Plug-in für SQL Server verwendet NetApp Snapshot Technologie mit dem NetApp SnapCenter Plug-in für Microsoft Windows. So können Sie Datenbanken in Sekundenschnelle sichern und schnell wiederherstellen, ohne SQL Server offline schalten zu müssen. Snapshots belegen nur minimalen Speicherplatz.

Zusätzlich zu diesen wichtigen Funktionen bietet das Plug-in für SQL Server folgende Vorteile:

- Unterstützung für Workflows für Backup, Wiederherstellung, Klonen und Verifizierung
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation
- Erstellung platzsparender und zeitpunktgenauer Kopien von Produktionsdatenbanken für Test- oder Datenextraktion mit der NetApp FlexClone Technologie

  Es ist eine FlexClone Lizenz auf dem Storage-System erforderlich, auf dem der Klon gespeichert ist.

- Unterbrechungsfreie und automatisierte Backup-Verifizierung
- Die Möglichkeit, mehrere Backups gleichzeitig über mehrere Server hinweg auszuführen
- PowerShell cmdlets zur Skripte von Backup-, Verifizierungs-, Wiederherstellungs- und Klonvorgängen
- Unterstützung von AlwaysOn Availability Groups (AGs) in SQL Server, um die Einrichtung, Backups und Restores von AGs zu beschleunigen

- In-Memory-Datenbank und Buffer Pool Extension (BPE) als Teil von SQL Server 2014
- Unterstützung von Backups von LUNs und Virtual Machine Disks (VMDKs)
- Unterstützung physischer und virtualisierter Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM) und VMDK über NFS und VMFS

> NAS Volumes sollten eine standardmäßige Exportrichtlinie in Storage Virtual Machine (SVM) verwenden.

- Unterstützung von FileStream und Dateigruppen in Standalone-Datenbanken von SQL Server
- Unterstützung für Non-Volatile Memory Express (NVMe) unter Windows Server 2022
  - Backup-, Restore-, Klon- und Verifizierungsworkflows auf VMDK-Layout, das auf NVMe over TCP/IP erstellt wurde.
  - Unterstützt NVMe-Firmware-Version 1.3 ab ESX 8.0 Update 2 und erfordert Virtual Hardware-Version 21.
  - Windows Server Failover Clustering (WSFC) wird nicht für Applikationen über VMDK auf NVMe over TCP/IP unterstützt.
- Unterstützung von SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Business Services auch bei einem vollständigen Standortausfall weiterlaufen können und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.

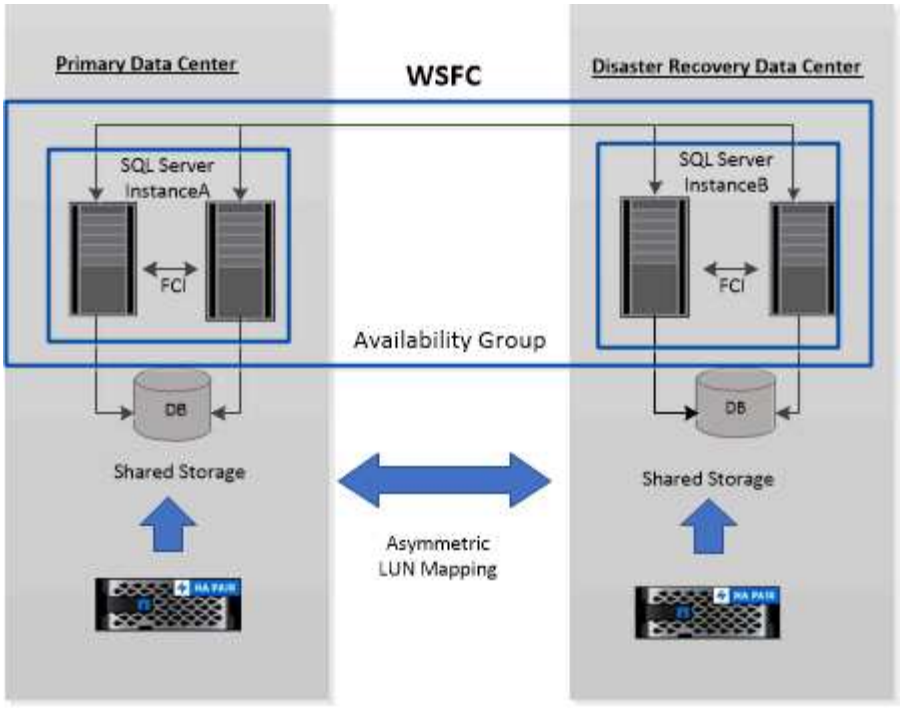
Unterstützung für asymmetrische LUN-Zuordnung in Windows Clustern

Das SnapCenter Plug-in für Microsoft SQL Server unterstützt die Erkennung in SQL Server 2012 und höher sowie ALM-Konfigurationen (Asymmetric LUN Mapping) für Hochverfügbarkeit und Verfügbarkeitsgruppen für Disaster Recovery. Bei der Ermittlung von Ressourcen erkennt SnapCenter Datenbanken auf lokalen Hosts und Remote-Hosts in ALM-Konfigurationen.

Eine ALM-Konfiguration ist ein einzelnes Windows Server Failover Cluster, das einen oder mehrere Nodes in einem primären Datacenter und einen oder mehrere Nodes in einem Disaster Recovery Center enthält.

Nachfolgend ein Beispiel für eine ALM-Konfiguration:

- Zwei Failover-Cluster-Instanzen (FCI) in einem Datacenter mit mehreren Standorten
- FCI für lokale Hochverfügbarkeit (HA) und Availability Group (AG) für Disaster Recovery mit Standalone-Instanz am Disaster-Recovery-Standort



WSFC----Windows Server Failover Cluster

Der Storage im primären Datacenter wird von den FCI-Nodes gemeinsam genutzt, die sich im primären Datacenter befinden. Der Storage im Disaster-Recovery-Datacenter wird von den FCI-Nodes geteilt, die sich im Disaster-Recovery-Datacenter befinden.

Der Storage im primären Datacenter ist für die Nodes im Disaster Recovery-Datacenter nicht sichtbar und umgekehrt.

ALM-Architektur kombiniert zwei von FCI verwendete Shared Storage-Lösungen mit einer nicht gemeinsam genutzten oder dedizierten Storage-Lösung, die von der SQL AG verwendet wird. Die AG Lösung verwendet identische Laufwerksbuchstaben für gemeinsam genutzte Festplattenressourcen über alle Datacenter hinweg. Diese Anordnung des Storage, bei der ein Cluster-Laufwerk von einem Teil der Nodes innerhalb eines WSFC gemeinsam genutzt wird, wird als ALM bezeichnet.

Vom SnapCenter-Plug-in für Microsoft SQL Server unterstützte Speichertypen

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines. Sie müssen überprüfen, ob Ihr Speichertyp unterstützt wird, bevor Sie das Paket für Ihren Host installieren.

SnapCenter Provisioning und Datensicherung werden unter Windows Server unterstützt. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische SnapCenter Benutzeroberfläche (GUI) oder PowerShell Commandlets	

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	ISCSI-verbundene LUNs	SnapCenter GUI oder PowerShell Commandlets	
Physischer Server	SMB3 (CIFS) Shares auf einer Storage Virtual Machine (SVM)	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung.
VMware VM	RDM-LUNs, die über einen FC- oder iSCSI-HBA verbunden sind	PowerShell Commandlets	
VMware VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	
VMware VM	Virtual Machine File Systems (VMFS) oder NFS-Datastores	VMware vSphere	
VMware VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung.
VMware VM	VVol Datastores auf NFS und SAN	ONTAP Tools für VMware vSphere	

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	Virtuelle FC-LUNs (VFC), die über einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Sie müssen Hyper-V Manager verwenden, um virtuelle FC (VFC) LUNs bereitzustellen, die über einen virtuellen Fibre Channel Switch verbunden sind.  Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.
Hyper-V VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	 Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Empfehlungen für das Storage-Layout für das SnapCenter Plug-in für Microsoft SQL Server

Mit dem gut durchdachten Storage-Layout kann SnapCenter Server Ihre Datenbanken entsprechend den Recovery-Vorgaben sichern. Bei der Definition des Storage-Layouts sollten Sie mehrere Faktoren berücksichtigen, darunter die Größe der Datenbank, die Änderungsrate der Datenbank und die Häufigkeit, mit der Sie Backups durchführen.

In den folgenden Abschnitten werden die Empfehlungen und Einschränkungen des Storage-Layouts für LUNs und Virtual Machine Disks (VMDKs) mit dem SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung definiert.

In diesem Fall können LUNs VMware RDM-Festplatten und die dem Gast zugeordneten iSCSI-Direct-Attached LUNs enthalten.

LUN- und VMDK-Anforderungen erfüllt

Sie können optional dedizierte LUNs oder VMDKs für eine optimale Performance und ein optimales Management für die folgenden Datenbanken verwenden:

- Master- und Modellsystemdatenbanken
- Tempdb
- Benutzerdatenbankdateien (.mdf und .ndf)
- Log-Dateien der Benutzerdatenbank-Transaktionen (.ldf)
- Protokollverzeichnis

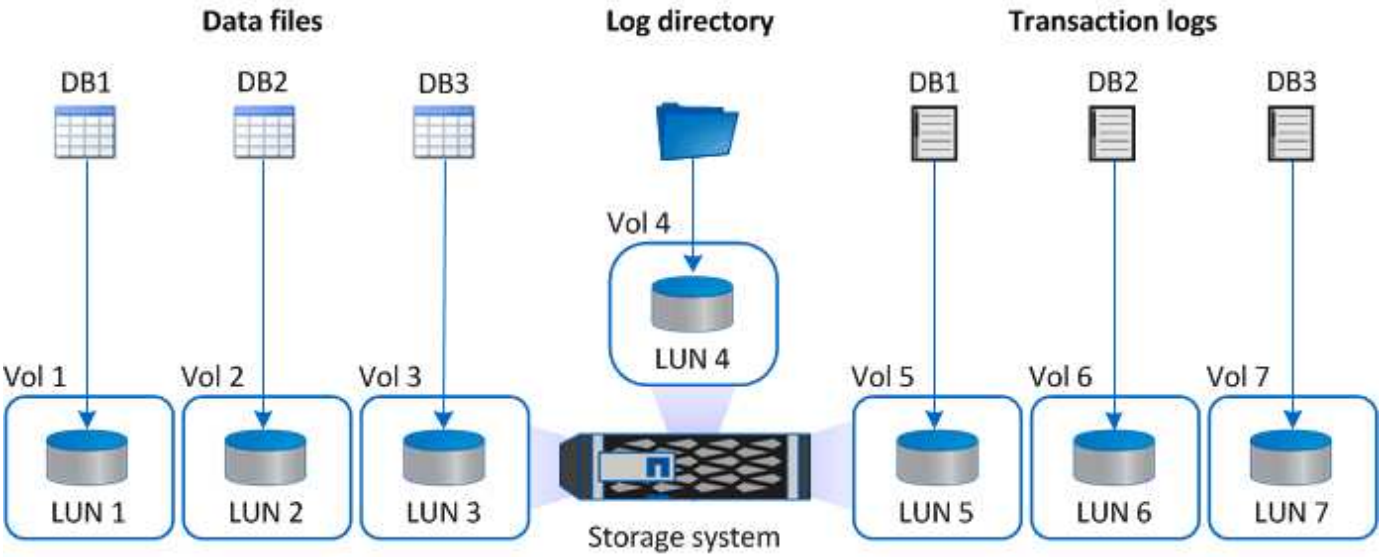
Zur Wiederherstellung großer Datenbanken empfiehlt es sich, dedizierte LUNs oder VMDKs zu verwenden. Die zur Wiederherstellung einer vollständigen LUN oder VMDK benötigte Zeit beträgt weniger als die Zeit zur

Wiederherstellung der in der LUN oder VMDK gespeicherten einzelnen Dateien.

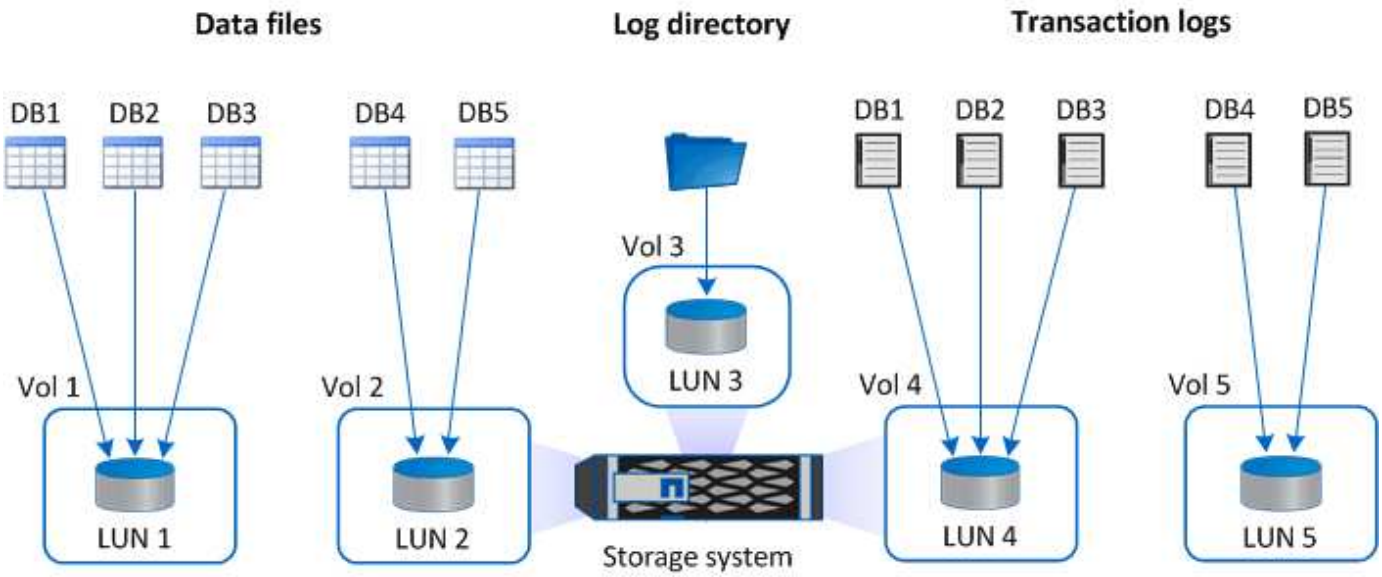
Für das Log-Verzeichnis sollten Sie eine separate LUN oder VMDK erstellen, damit genügend freier Speicherplatz in den Daten- oder Log-Datei-Disks vorhanden ist.

Beispiellayouts für LUN und VMDK

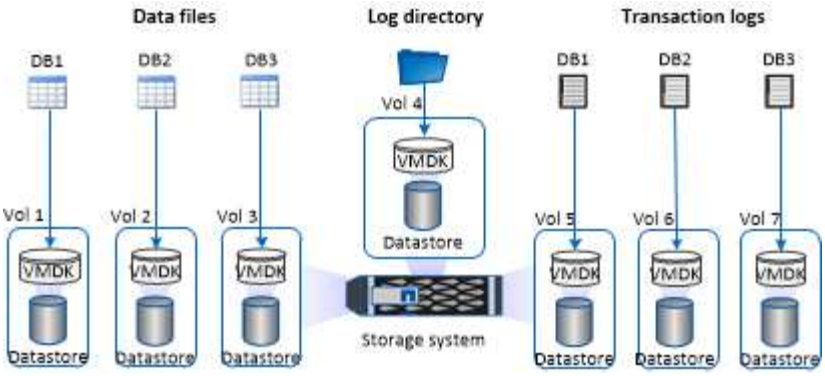
Die folgende Grafik zeigt, wie Sie das Storage-Layout für große Datenbanken auf LUNs konfigurieren können:



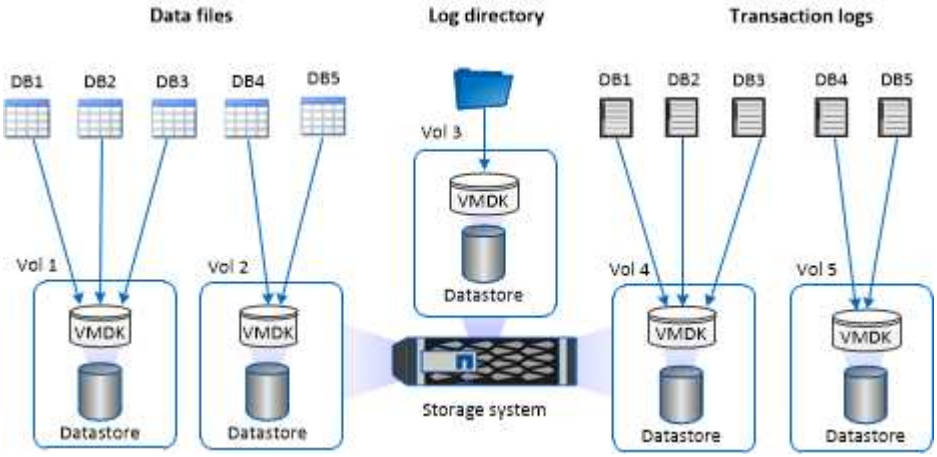
Die folgende Grafik zeigt, wie Sie das Storage-Layout für mittelgroße oder kleine Datenbanken auf LUNs konfigurieren können:



Die folgende Grafik zeigt, wie Sie das Storage-Layout für große Datenbanken auf VMDKs konfigurieren können:



Die folgende Grafik zeigt, wie Sie das Storage-Layout für mittelgroße oder kleine Datenbanken auf VMDKs konfigurieren können:



Minimale ONTAP-Berechtigungen für SQL Plug-in erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun erstellen
  - lun löschen
  - lun Initiatorgruppe hinzufügen
  - lun-Initiatorgruppe wird erstellt
  - lun-Initiatorgruppe löschen
  - lun igroup umbenennen
  - lun-Initiatorgruppe wird angezeigt
  - lun Mapping Add-Reporting-Nodes
  - lun-Zuordnung erstellen

- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen
- Show-Disk-Nutzung für Volume-Dateien
- Volume ist offline
- Das Volume ist online
- Volume-Änderung
- Erstellen von Volume-qtree
- Volume qtree löschen
- Änderung des Volume-qtree
- Volume-qtree anzeigen
- Volume-Einschränkung

- Volumen anzeigen
- Erstellen von Volume-Snapshots
- Volume Snapshot löschen
- Ändern des Volume-Snapshots
- Umbenennung von Volume-Snapshots
- Wiederherstellung von Volume Snapshots
- Restore-Datei für Volume Snapshots
- Volume-Snapshot werden angezeigt
- Volume-Aufhängung nicht verfügbar
- cifs von vserver
- erstellung von cifs-Freigaben von vserver
- cifs-Freigabe von vserver: Löschen
- vserver cifs shadowcopy anzeigen
- cifs-Freigabe von vserver wird angezeigt
- vserver cifs zeigen
- vserver Exportrichtlinie
- Erstellung von vserver Exportrichtlinien
- vserver: Löschen der Exportrichtlinie
- Erstellung von vserver Export-Policy-Regel
- vserver: Export-Policy-Regel anzeigen
- vserver Export-Policy wird angezeigt
- vserver iscsi
- vserver iscsi-Verbindung wird angezeigt
- vserver zeigen
- Netzwerkschnittstelle
- Netzwerkschnittstelle wird angezeigt
- vserver
- MetroCluster zeigen

Storage-Systeme für SnapMirror und SnapVault Replizierung für Plug-in für SQL Server vorbereiten

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang

abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie für SQL Server-Ressourcen

Backup-Strategie für SQL Server-Ressourcen definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, können Sie sicherstellen, dass Sie über die Backups verfügen, die Sie benötigen, um Ihre Datenbanken erfolgreich wiederherzustellen oder zu klonen. Ihre Backup-Strategie wird durch Ihre Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) weitgehend bestimmt.

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Die RTO ist der Zeitpunkt, zu dem ein Geschäftsprozess nach einer Service-Unterbrechung wiederhergestellt werden muss. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Backup-Strategie bei.

Art der unterstützten Backups

Für das Sichern des SQL Server-Systems und der Benutzerdatenbanken mit SnapCenter müssen Sie den Ressourcentyp auswählen, z. B. Datenbanken, SQL Server-Instanzen und Verfügbarkeitsgruppen (AG). Mithilfe der Snapshot Technologie werden schreibgeschützte Online-Kopien der Volumes erstellt, auf denen sich die Ressourcen befinden.

Sie können die Option nur kopieren auswählen, um anzugeben, dass der SQL-Server die Transaktionsprotokolle nicht schneidet. Sie sollten diese Option verwenden, wenn Sie auch SQL Server mit anderen Backup-Anwendungen verwalten. Wenn die Transaktionsprotokolle intakt bleiben, kann jede Backup-Anwendung die Systemdatenbanken wiederherstellen. Backups, bei denen nur Kopien erstellt werden, sind unabhängig von der Sequenz geplanter Backups und haben keine Auswirkungen auf die Backup- und Restore-Vorgänge der Datenbank.

Backup-Typ	Beschreibung	Copy-Only-Option mit Backup-Typ
Vollständiges Backup und Backup von Protokollen	Sichert die Systemdatenbank und schneidet die Transaktionsprotokolle ab. Der SQL Server schneidet die Transaktionsprotokolle ab, indem die Einträge entfernt werden, die bereits in der Datenbank gespeichert sind. Nach Abschluss der vollständigen Sicherung erstellt diese Option ein Transaktionsprotokoll, das die Transaktionsinformationen erfasst. Normalerweise sollten Sie diese Option wählen. Wenn Ihre Backup-Zeit jedoch kurz ist, können Sie wählen, keine Transaktions-Log-Backup mit vollständiger Sicherung auszuführen. Sie können keine Protokollsicherung für Master- und msdb-Systemdatenbanken erstellen. Sie können jedoch Protokoll-Backups für Modell-System-Datenbank erstellen.	Sichert die Systemdatenbankdateien und die Transaktions-Logs, ohne die Protokolle zu beeinträchtigen. Ein Backup nur für Kopien kann nicht als differenzielles Basis- oder differenzielles Backup dienen und hat keine Auswirkungen auf die Differentialbasis. Die Wiederherstellung eines nur-Kopie-Vollbackups ist mit der Wiederherstellung eines anderen vollständigen Backups identisch.
Vollständiges Datenbank-Backup	Sichert die Systemdatenbankdateien. Sie können vollständige Datenbank-Backup für Master-, Modell- und msdb-Systemdatenbanken erstellen.	Sichert die Systemdatenbankdateien.
Transaktions-Log-Backup	Sichert die gekürzten Transaktionsprotokolle, kopiert nur die Transaktionen, die seit dem letzten Transaktions-Log gesichert wurden. Wenn Sie häufige Transaktions-Log-Backups neben vollständigen Datenbank-Backups planen, können Sie granulare Recovery-Punkte auswählen.	Sicherung der Transaktions-Logs, ohne sie zu beeinträchtigen Diese Sicherungsart hat keine Auswirkung auf die Sequenzierung von regelmäßigen Protokollsicherungen. Backups nur-Kopien-Protokolle sind für die Durchführung von Online-Wiederherstellungen nützlich.

Backup-Pläne für Plug-in für SQL Server

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen. So könnten beispielsweise regelmäßige Transaktions-Log-Backups ausreichen, um sicherzustellen, dass Sie die Backups haben, die Sie benötigen. Je öfter Sie Ihre Datenbanken sichern, desto weniger Transaktions-Logs benötigt SnapCenter zum Zeitpunkt der Wiederherstellung, was zu schnelleren Restore-Vorgängen führen kann.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Backups konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Datenbanken erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Datenbank, die Anzahl der verwendeten Volumes, die Änderungsrate der Datenbank und Ihr Service Level Agreement (SLA).

Die Anzahl der von Ihnen gewählten Backup-Aufgaben hängt bei Datenbank-Backups in der Regel von der Anzahl der Volumes ab, auf denen Sie Ihre Datenbanken platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Datenbanken auf einem Volume und einer großen Datenbank auf einem anderen Volume platziert haben, können Sie einen Backup-Job für die kleinen Datenbanken und einen Backup-Job für die große Datenbank erstellen.

Backup-Namenskonventionen für SQL Server

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Optionen zur Backup-Aufbewahrung für Plug-in für SQL Server

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Wie lange werden Transaktions-Log-Backups auf dem Quell-Storage-System aufbewahrt

Das SnapCenter Plug-in für Microsoft SQL Server benötigt Transaktions-Log-Backups, um minutengenaue Restore-Vorgänge durchzuführen, bei denen Ihre Datenbank zwischen zwei vollständigen Backups wiederhergestellt wird.

Wenn zum Beispiel Plug-in für SQL Server um 8:00 Uhr ein vollständiges Backup und um 5:00 Uhr ein weiteres komplettes Backup erstellt hat, könnte es die letzte Sicherung des Transaktionsprotokolls verwenden, um die Datenbank zwischen 8:00 Uhr und 5:00 Uhr wiederherzustellen. Wenn Transaktionsprotokolle nicht verfügbar sind, das Plug-in für SQL Server kann nur Point-in-Time-Wiederherstellungsvorgänge durchführen, die eine Datenbank so lange wiederherstellen, wie das Plug-in für SQL Server ein vollständiges Backup abgeschlossen hat.

In der Regel erfordern Sie minutengenaue Restore-Vorgänge nur für einen oder zwei Tage. SnapCenter speichert standardmäßig mindestens zwei Tage.

Mehrere Datenbanken auf demselben Volume

Sie können alle Datenbanken auf demselben Volume ablegen, da die Backup-Richtlinie die Möglichkeit hat, die maximale Datenbank pro Backup festzulegen (Standardwert ist 100).

Wenn Sie beispielsweise 200 Datenbanken auf demselben Volume haben, werden zwei Snapshots mit 100 Datenbanken in jedem der beiden Snapshots erstellt.

Verifizierung von Backup-Kopien für SQL Server mithilfe des primären oder sekundären Storage Volumes

Sie können Backup-Kopien auf dem primären Storage Volume oder auf dem sekundären SnapMirror oder SnapVault Storage Volume überprüfen. Bei der Überprüfung und Verwendung eines sekundären Storage-Volumes wird die Last für das primäre Storage Volume verringert.

Wenn Sie ein Backup überprüfen, das sich entweder auf dem primären oder sekundären Storage-Volume befindet, werden alle primären und sekundären Snapshots als verifiziert markiert.

Zur Überprüfung von Backup-Kopien auf dem sekundären SnapVault Storage Volume ist eine SnapRestore Lizenz erforderlich.

Wann werden Überprüfungsaufträge geplant

SnapCenter kann Backups zwar sofort nach der Erstellung überprüfen, kann aber die zum Abschließen des Backup-Jobs erforderliche Zeit erheblich verlängern und ist ressourcenintensiv. Daher ist es fast immer am besten, die Verifizierung in einem separaten Job für ein späteres Mal zu planen. Wenn Sie beispielsweise jeden Tag um 5:00 Uhr ein Backup einer Datenbank erstellen, können Sie die Überprüfung möglicherweise eine Stunde später um 6:00 Uhr planen

Aus dem gleichen Grund ist es in der Regel nicht erforderlich, die Backup-Verifizierung jedes Mal, wenn Sie ein Backup ausführen. Eine Überprüfung in regelmäßigen, aber weniger häufigen Abständen durchzuführen, reicht normalerweise aus, um die Integrität des Backups zu gewährleisten. Ein einziger Verifizierungsauftrag

kann mehrere Backups gleichzeitig überprüfen.

Wiederherstellungsstrategie für SQL Server

Definieren einer Wiederherstellungsstrategie für SQL Server

Durch die Definition einer Wiederherstellungsstrategie für SQL Server können Sie Ihre Datenbank erfolgreich wiederherstellen.

Quellen und Ziele für einen Wiederherstellungsvorgang

Sie können eine SQL Server Datenbank aus einer Backup-Kopie auf einem primären oder sekundären Storage wiederherstellen. Sie können die Datenbank zusätzlich zum ursprünglichen Speicherort auch an verschiedenen Zielen wiederherstellen, sodass Sie das Ziel auswählen können, das Ihre Anforderungen unterstützt.

Quellen für einen Wiederherstellungsvorgang

Sie können Datenbanken aus primärem oder sekundärem Storage wiederherstellen.

Ziele für einen Wiederherstellungsvorgang

Sie können Datenbanken an verschiedenen Zielen wiederherstellen:

Ziel	Beschreibung
Der ursprüngliche Standort	Standardmäßig stellt SnapCenter die Datenbank an demselben Speicherort auf derselben SQL Serverinstanz wieder her.
Ein anderer Ort	Sie können die Datenbank an einem anderen Ort auf einer beliebigen SQL Server-Instanz innerhalb desselben Hosts wiederherstellen.
Ursprünglicher oder anderer Speicherort unter Verwendung unterschiedlicher Datenbanknamen	Sie können die Datenbank mit einem anderen Namen als jede SQL Server-Instanz auf demselben Host wiederherstellen, auf dem das Backup erstellt wurde.

Wiederherstellung eines alternativen Hosts über ESX Server für SQL-Datenbanken auf VMDKs (NFS- und VMFS-Datastores) wird nicht unterstützt.

Von SnapCenter unterstützte SQL Server Recovery-Modelle

Jedem Datenbanktyp werden standardmäßig spezifische Recovery-Modelle zugewiesen. Der SQL Server Datenbankadministrator kann jede Datenbank einem anderen Recovery-Modell zuweisen.

SnapCenter unterstützt drei Arten von SQL Server Recovery-Modellen:

- Einfaches Recovery-Modell

Wenn Sie das einfache Wiederherstellungsmodell verwenden, können Sie keine Backups der Transaktions-Logs erstellen.

- Vollständiges Recovery-Modell

  Wenn Sie das vollständige Recovery-Modell verwenden, können Sie eine Datenbank vom Zeitpunkt eines Ausfalls auf ihren vorherigen Zustand wiederherstellen.

- Recovery-Modell mit Massenprotokollierter

  Wenn Sie das Recovery-Modell mit der Massenprotokollierfunktion verwenden, müssen Sie den protokollierten Massenvorgang manuell erneut ausführen. Sie müssen den protokollierten Massenvorgang durchführen, wenn das Transaktionsprotokoll, das den Verschiebdatensatz des Vorgangs enthält, vor der Wiederherstellung nicht gesichert wurde. Wenn der Bulk Logged-Vorgang 10 Millionen Zeilen in eine Datenbank einfügt und die Datenbank vor dem Backup des Transaktionsprotokolls ausfällt, enthält die wiederhergestellte Datenbank nicht die Zeilen, die von der protokollierten Massenoperation eingefügt wurden.

Arten von Wiederherstellungsvorgängen

Sie können SnapCenter verwenden, um verschiedene Arten von Wiederherstellungsvorgängen auf SQL Server-Ressourcen durchzuführen.

- Wiederherstellung im Minutenschnoch
- Wiederherstellung auf einen früheren Zeitpunkt

In den folgenden Situationen lassen sich Wiederherstellungen bis zur Minute durchführen oder ein Recovery auf einen früheren Zeitpunkt durchführen:

- Wiederherstellung aus sekundärem SnapMirror oder SnapVault Storage
- Wiederherstellung auf alternativem Pfad (Speicherort)

SnapCenter bietet keine Unterstützung für Volume-basierte SnapRestore.

Führen Sie Wiederherstellungen minutengenau durch

In einem up-to-the-minute-Wiederherstellungsvorgang (standardmäßig ausgewählt) werden Datenbanken bis zum Fehlerpunkt wiederhergestellt. SnapCenter erreicht dies durch folgende Sequenz:

1. Sichert das letzte aktive Transaktionsprotokoll vor dem Wiederherstellen der Datenbank.
2. Stellt die Datenbanken aus dem vollständigen Datenbank-Backup wieder her, das Sie auswählen.
3. Wendet alle Transaktionsprotokolle an, die nicht den Datenbanken zugeschrieben wurden (einschließlich Transaktions-Logs aus den Backups vom Zeitpunkt der Erstellung des Backups bis zum aktuellsten Zeitpunkt).

   Transaktionsprotokolle werden nach vorne verschoben und auf alle ausgewählten Datenbanken angewendet.

Für eine minutengenaue Wiederherstellung ist ein zusammenhängender Satz von Transaktionsprotokollen erforderlich.

Da der SnapCenter die Transaktionsprotokolle der SQL Server-Datenbank nicht aus den Log-shipping Backup-Dateien wiederherstellen kann (durch die Protokollversand können Sie Transaktions-Log-Backups automatisch von einer primären Datenbank auf einer primären Serverinstanz an eine oder mehrere sekundäre Datenbanken auf separaten sekundären Serverinstanzen senden), Sie können keine up-to-the-minute-Wiederherstellung aus den Transaktions-Log-Backups durchführen. Aus diesem Grund sollten Sie den SnapCenter verwenden, um Ihre Transaktions-Log-Dateien für die SQL Server-Datenbank zu sichern.

Wenn Sie keine up-to-the-minute-Wiederherstellung für alle Backups benötigen, können Sie die Transaktions-Log-Backup-Aufbewahrung Ihres Systems mithilfe der Backup-Richtlinien konfigurieren.

Beispiel für einen minutengenauen Restore-Vorgang

Nehmen wir an, dass Sie das SQL Server-Backup täglich um 12.00 Uhr und am Mittwoch um 4:00 Uhr von einem Backup aus ausführen müssen. Aus irgendeinem Grund, die Sicherung von Mittwoch Mittag nicht überprüft, so entscheiden Sie sich für die Wiederherstellung von Dienstag Mittag Backup. Wenn das Backup wiederhergestellt ist, werden alle Transaktionsprotokolle nach vorne verschoben und auf die wiederhergestellten Datenbanken angewendet. Dies beginnt mit den Daten, die nicht bei der Erstellung des Backups am Dienstag festgelegt wurden, und es wird das letzte Transaktionsprotokoll, das am Mittwoch um 4:00 Uhr geschrieben wurde, fortgesetzt (wenn die Transaktions-Logs gesichert wurden).

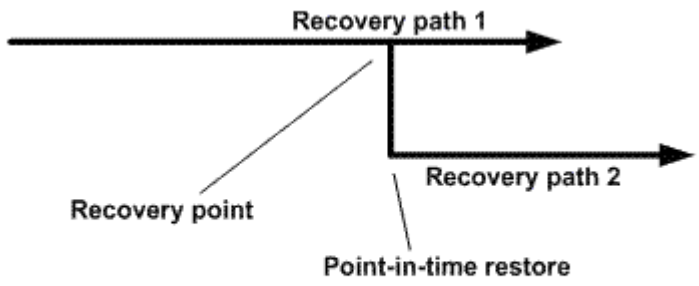
Wiederherstellung auf einen früheren Zeitpunkt

In einer zeitpunktgenauen Restore-Operation werden Datenbanken nur auf eine bestimmte Zeit aus der Vergangenheit wiederhergestellt. Ein Point-in-Time-Wiederherstellungsvorgang findet in den folgenden Situationen statt:

- Die Datenbank wird zu einem bestimmten Zeitpunkt in einem gesicherten Transaktions-Log wiederhergestellt.
- Die Datenbank ist wiederhergestellt, und nur ein Teil der gesicherten Transaktions-Logs wird angewendet.

Durch das Wiederherstellen einer Datenbank zu einem bestimmten Zeitpunkt wird ein neuer Recovery-Pfad benötigt.

Die folgende Abbildung zeigt die Probleme bei der Durchführung eines Point-in-Time-Restore-Vorgangs:



Im Image besteht der Recovery-Pfad 1 aus einem kompletten Backup gefolgt von mehreren Transaktions-Log-Backups. Sie stellen die Datenbank zu einem bestimmten Zeitpunkt wieder her. Nach dem zeitpunktgenauen Restore werden neue Transaktions-Log-Backups erstellt, was Recovery-Pfad 2 zur Folge hat. Die neuen Transaktions-Log-Backups werden ohne neue vollständige Sicherung erstellt. Aufgrund von Datenbeschädigungen oder anderen Problemen können Sie die aktuelle Datenbank nicht wiederherstellen, bis ein neues vollständiges Backup erstellt wird. Darüber hinaus ist es nicht möglich, die in Recovery-Pfad 2

erstellten Transaktionsprotokolle auf das vollständige Backup des Recovery-Pfads 1 anzuwenden.

Wenn Sie Backups des Transaktionsprotokolls anwenden, können Sie auch ein bestimmtes Datum und eine bestimmte Uhrzeit angeben, zu der Sie die Anwendung der gesicherten Transaktionen beenden möchten. Dazu geben Sie ein Datum und eine Uhrzeit innerhalb des verfügbaren Bereichs an, und der SnapCenter entfernt alle Transaktionen, die vor diesem Zeitpunkt nicht durchgeführt wurden. Mit dieser Methode können Sie Datenbanken bis zu einem Zeitpunkt vor einer Beschädigung wiederherstellen oder nach einer versehentlichen Datenbank- oder Tabellenlöschung wiederherstellen.

Beispiel für einen Point-in-Time Restore-Vorgang

Angenommen, Sie erstellen um Mitternacht volle Datenbank-Backups und ein Transaktions-Log-Backup jede Stunde. Die Datenbank stürzt um 9:45 Uhr ab, aber Sie sichern immer noch die Transaktionsprotokolle der fehlgeschlagenen Datenbank. Es stehen folgende Point-in-Time-Wiederherstellungsszenarien zur Auswahl:

- Stellen Sie das vollständige Datenbank-Backup um Mitternacht wieder her und akzeptieren Sie den Verlust der danach vorgenommenen Datenbankänderungen. (Option: Keine)
- Stellen Sie die vollständige Datenbanksicherung wieder her, und wenden Sie alle Transaktionsprotokollsicherungen bis 9:45 Uhr an (Option: Protokoll bis).
- Stellen Sie die vollständige Datenbank-Sicherung wieder her und wenden Sie Transaktions-Log-Backups an. Geben Sie dabei die Zeit an, die die Transaktionen von den letzten Transaktions-Log-Backups wiederherstellen 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 vor dem angegebenen Datum und der angegebenen Uhrzeit nicht begangen wurden, werden entfernt.

Definieren Sie eine Klonstrategie für SQL Server

Wenn Sie eine Klonstrategie definieren, können Sie Ihre Datenbank erfolgreich klonen.

1. Prüfen Sie die Einschränkungen hinsichtlich von Klonvorgängen.
2. Legen Sie den für Sie erforderlichen Klontyp fest.

Einschränkungen von Klonvorgängen

Die Einschränkungen von Klonvorgängen sollten Sie beachten, bevor Sie die Datenbanken klonen.

- Wenn Sie eine Oracle-Version von 11.2.0.4 bis 12.1.0.1 verwenden, befindet sich der Klonvorgang im Status „Hung“, wenn Sie den Befehl „*renamedg*“ ausführen. Sie können den Oracle Patch 19544733 anwenden, um dieses Problem zu beheben.
- Das Klonen von Datenbanken aus einem LUN, die direkt an einen Host angebunden ist (z. B. durch die Verwendung von Microsoft iSCSI Initiator auf einem Windows Host), wird auf demselben Windows Host oder einem anderen Windows Host oder umgekehrt nicht unterstützt.
- Das Stammverzeichnis des Volume-Bereitstellungspunkts kann kein freigegebenes Verzeichnis sein.
- Wenn Sie eine LUN verschieben, die einen Klon in ein neues Volume enthält, kann der Klon nicht gelöscht werden.

Typen von Klonvorgängen

Sie können SnapCenter verwenden, um ein Backup einer SQL Server Datenbank oder eine Produktionsdatenbank zu klonen.

- Klonen aus einem Datenbank-Backup

  Die geklonte Datenbank kann als Basis für die Entwicklung neuer Applikationen dienen und Applikationsfehler isolieren, die in der Produktionsumgebung auftreten. Die geklonte Datenbank kann auch für das Recovery nach Fehlern bei Datenbanken verwendet werden.

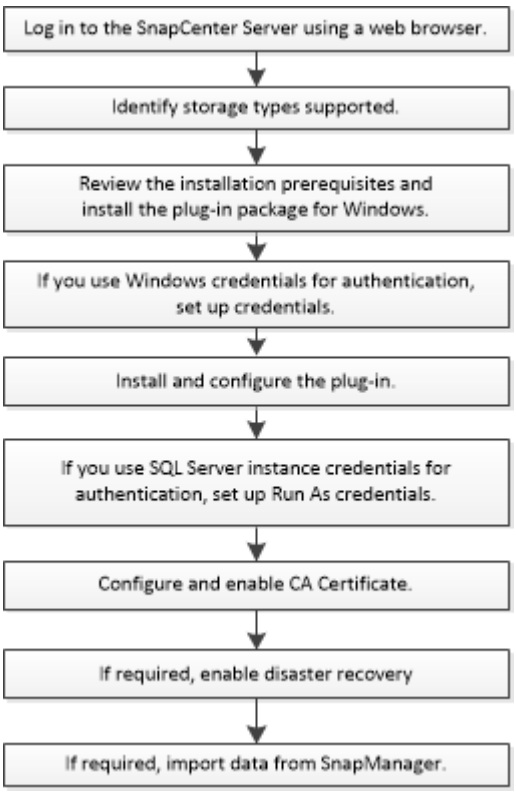
- Lebenszyklus von Klonen

  Sie können SnapCenter verwenden, um wiederkehrende Klonjobs zu planen, die auftreten, wenn die Produktionsdatenbank nicht beschäftigt ist.

Bereiten Sie die Installation des SnapCenter-Plug-ins für Microsoft SQL Server vor

Installations-Workflow 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 für das Hinzufügen von Hosts und die Installation des SnapCenter-Plug-ins für Microsoft SQL Server

Bevor Sie einen Host hinzufügen und die Plug-ins-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 mit lokalen Anmeldeberechtigungen auf

dem Remote-Host verfügen.

- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen über einen Benutzer mit sysadmin-Berechtigungen auf dem SQL Server verfügen.

  Das SnapCenter Plug-in für Microsoft SQL Server verwendet Microsoft VDI Framework, für das ein sysadmin-Zugriff erforderlich ist.

  "Microsoft Support-Artikel 2926557: Für Backup- und Restore-Vorgänge für SQL Server VDI sind Sysadmin-Berechtigungen erforderlich"

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Wenn SnapManager für Microsoft SQL Server installiert ist, müssen Sie den Service und die Zeitpläne angehalten oder deaktiviert haben.

  Wenn Sie Backup- oder Klonaufträge in SnapCenter importieren möchten, deinstallieren Sie SnapManager für Microsoft SQL Server nicht.

- Der Host muss auf den vollständig qualifizierten Domänennamen (FQDN) vom Server resolable sein.

  Wenn die Host-Datei geändert wird, damit sie resolable ist, und wenn sowohl der Kurzname als auch der FQDN in der Datei Hosts angegeben sind, erstellen Sie einen Eintrag in der Datei SnapCenter Hosts im folgenden Format: <ip_Address> <Host_fqdn> <Host_Name>

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-ins-Paket für Windows ein

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken oder Windows-Dateisystemen erstellen.

Bevor Sie beginnen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.
- Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.
- SQL-Authentifizierung auf Windows Hosts

  Nach der Installation von Plug-ins müssen Sie SQL-Anmeldedaten einrichten.

  Wenn Sie SnapCenter-Plug-in für Microsoft SQL Server bereitstellen, müssen Sie nach der Installation von

Plug-ins SQL-Anmeldedaten einrichten. Richten Sie eine Anmeldedaten für einen Benutzer mit den sysadmin-Berechtigungen von SQL Server ein.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domain-Administrator Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld Benutzername lautet: `UserName` Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
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 einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Konfigurieren von Anmeldeinformationen für eine einzelne SQL Server-Ressource

Sie können Anmeldedaten für die Durchführung von Datensicherungsjobs für einzelne SQL Server-Ressourcen für jeden Benutzer konfigurieren. Sie können die

Anmeldeinformationen zwar global konfigurieren, aber dies ist möglicherweise nur für eine bestimmte Ressource erforderlich.

Über diese Aufgabe

- Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie vor der Installation von Plug-ins die Anmeldedaten einrichten.

  Wenn Sie jedoch eine SQL Server-Instanz zur Authentifizierung verwenden, müssen Sie nach der Installation von Plug-ins die Anmeldeinformationen hinzufügen.

- Wenn Sie die SQL-Authentifizierung beim Einrichten der Anmeldeinformationen aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Farbvorhängeschloss-Symbol angezeigt.

  Wenn das Vorhängeschloss-Symbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, um die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzuzufügen.

- Sie müssen die Anmeldedaten einem Benutzer mit rollenbasierter Zugriffssteuerung (Role-Based Access Control, RBAC) ohne sysadmin-Zugriff 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 Ressourcengruppe als auch über die Sicherungsberechtigungen verfügen.

Schritt 1: Anmeldeinformationen hinzufügen und konfigurieren

1. Wählen Sie im linken Navigationsbereich **Einstellungen**.
2. Wählen Sie auf der Seite Einstellungen die Option **Credential** aus.
   a. Um eine neue Anmeldeinformation hinzuzufügen, wählen Sie **Neu**.
   b. Konfigurieren Sie auf der Seite Anmeldeinformationen:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen ein, der für die SQL Server-Authentifizierung verwendet wird. • Domänenadministrator oder ein Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld **Benutzername** sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld **Benutzername** lautet: *Username*
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den SQL Server-Authentifizierungsmodus aus. Sie können auch die Windows-Authentifizierung auswählen, wenn der Windows-Benutzer sysadmin-Berechtigungen auf dem SQL-Server hat.
Host	Wählen Sie den Host aus.
SQL Server Instanz	Wählen Sie die SQL Server-Instanz aus.

c. Wählen Sie **OK**, um die Zugangsdaten hinzuzufügen.

Schritt 2: Instanzen konfigurieren

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Instanz** aus.
   a. Wählen Sie Image::../media/Filter_icon.png[Filter icon] aus, und wählen Sie dann den Hostnamen aus, um die Instanzen zu filtern.
   b. Wählen Sie Bild::../media/Filter_icon.png[Filtersymbol] aus, um den Filterbereich zu schließen.
3. Schützen Sie die Instanz auf der Seite Instance Protect, und wählen Sie bei Bedarf **Credentials konfigurieren**.

   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 Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Installieren Sie das SnapCenter Plug-in für Microsoft SQL Server

Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Windows

Sie müssen die Seite SnapCenter **Add Host** verwenden, um Hosts hinzuzufügen und das Plug-ins-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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, sollten Sie UAC auf dem Host deaktivieren, wenn Sie keine integrierten Anmeldeinformationen angeben.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange in Betrieb ist.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2016 oder höher für SQL"

Über diese Aufgabe

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 "Management von Hosts".

Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie Windows als Hosttyp aus. Der SnapCenter-Server fügt den Host hinzu und installiert dann das Plug-in für Windows, wenn das Plug-in nicht bereits auf dem Host installiert ist. Wenn Sie auf der Seite Plug-ins die Option Microsoft SQL Server auswählen, installiert der SnapCenter-Server das Plug-in für SQL Server.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. Die IP-Adresse wird nur für nicht vertrauenswürdige Domänenhosts unterstützt, wenn sie auf den FQDN auflöst. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • WSFC Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomain ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie den Anmeldeinformationsnamen aus, den Sie erstellt haben oder neue Anmeldeinformationen erstellen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

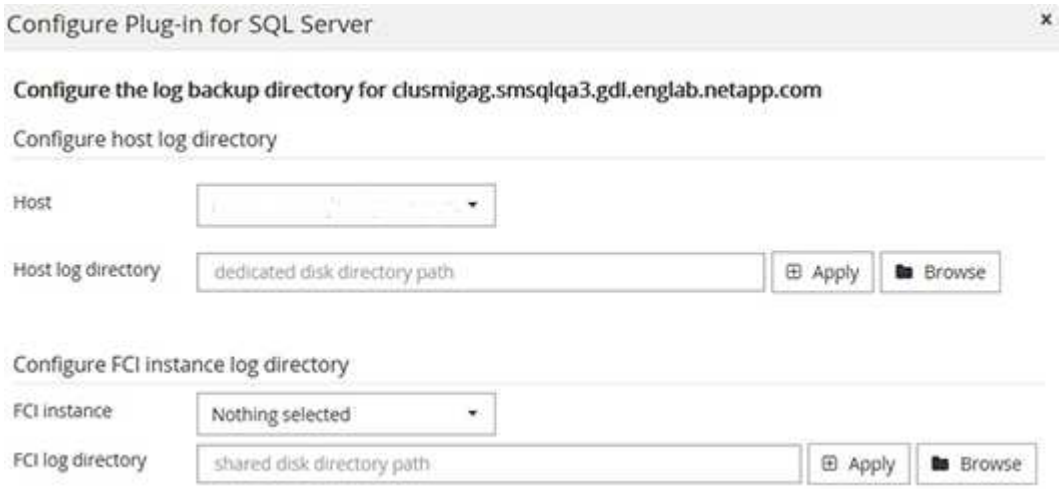
5. Wählen Sie im Abschnitt **Plug-ins zur Installation auswählen** die zu installierenden Plug-ins aus.
6. Wählen Sie **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist C:\Programmdateien\NetApp\SnapCenter. Optional können Sie den Pfad anpassen.
Fügen Sie alle Hosts im Cluster hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einer WSFC- oder SQL-Verfügbarkeitsgruppe hinzuzufügen. Sie sollten alle Cluster-Knoten hinzufügen, indem Sie das entsprechende Kontrollkästchen Cluster in der GUI aktivieren, wenn Sie mehrere verfügbare SQL-Verfügbarkeitsgruppen in einem Cluster verwalten und identifizieren möchten.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und sys Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

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 Hostprotokoll konfigurieren **Durchsuchen** aus, und führen Sie die folgenden Schritte aus:

      Nur NetApp LUNs (Laufwerke) werden zur Auswahl aufgeführt. SnapCenter sichert und repliziert im Rahmen des Backup-Vorgangs das Host-Protokollverzeichnis.



      i. Wählen Sie den Laufwerksbuchstaben oder den Bereitstellungspunkt auf dem Host aus, auf dem das Hostprotokoll gespeichert werden soll.
      ii. Wählen Sie ggf. ein Unterverzeichnis aus.
      iii. Wählen Sie **Speichern**.
9. Wählen Sie **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. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden mit den Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\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 Remote Hosts

Sie können das SnapCenter-Plug-in für Microsoft SQL Server auf mehreren Hosts gleichzeitig installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das SnapCenter-Plug-in für Microsoft SQL Server auf mehreren Remote-Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

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

   Sie können die Option -skipprecheck 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 Benutzeroberfläche von SnapCenter installieren. Wenn Sie jedoch aus irgendeinem Grund nicht in der Lage sind, das Installationsprogramm Plug-in für SQL Server unbeaufsichtigt im Silent-Modus von der Windows-Befehlszeile aus auszuführen.

Bevor Sie beginnen

- Vor der Installation müssen Sie die frühere Version des SnapCenter-Plug-ins für Microsoft SQL Server löschen.

  Weitere Informationen finden Sie unter "So installieren Sie ein SnapCenter-Plug-in manuell und direkt über den 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 SQL Server unter C:\ProgramData\NetApp\SnapCenter\Package Repository herunter.

   Auf diesen Pfad kann von dem Host 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 zum Verzeichnis, in das Sie die Plug-in-Installationsdateien gespeichert haben.
5. Installieren Sie das Plug-in für SQL Server:

```
"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 für das Installationsprogramm der Suite.
- Log_Path ist der Speicherort der Installationsprotokolle der Plug-in-Komponenten (SCW, SCSCSQL und SMCore).
- Num ist der Port, an dem SnapCenter mit SMCore kommuniziert
- Install_Directory_Path ist das Installationsverzeichnis des Host-Plug-in-Pakets.
- Domain\Administrator ist das SnapCenter-Plug-in für Microsoft Windows-Webservice-Konto.
- Passwort ist das Passwort für das SnapCenter-Plug-in für Microsoft Windows Webservice-Konto.

```
"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 der Installation von Plug-in für SQL Server müssen alle Parameter beachtet werden.

6. Überwachen Sie den Windows Task Scheduler, die Hauptinstallationsprotokolldatei C:\Installdebug.log und die zusätzlichen Installationsdateien in C:\Temp.
7. Überwachen Sie das Verzeichnis %temp%, um zu überprüfen, ob die msiexe.exe Installationsprogramme fehlerfrei installiert werden.

Die Installation des Plug-ins für SQL Server registriert das Plug-in auf dem Host und nicht auf dem SnapCenter-Server. Sie können das Plug-in auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Nach dem Hinzufügen des Hosts 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 über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

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

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

Schritte

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.

3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
    a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

       Get-ChildItem -Path Cert:\LocalMachine\My

    b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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"
   ```

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Konfiguration der Disaster Recovery

Disaster Recovery eines SnapCenter Plug-ins für SQL Server

Wenn das SnapCenter-Plug-in für SQL Server ausfällt, 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 das gleiche Betriebssystem, die gleiche Anwendung und den gleichen Hostnamen wie der primäre Host haben.
- Schieben Sie das SnapCenter-Plug-in für SQL Server auf einen anderen Host, indem Sie die Seite **Add Host** oder **Modify Host** verwenden. Weitere Informationen finden Sie unter "Management von Hosts" .

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 das SnapCenter-Plug-in für SQL Server-Konfigurationsdateien vom Disaster Recovery-Backup (DR) auf die neue Maschine.

3. Importieren Sie Windows- und SQL-Zeitpläne aus dem SnapCenter-Plug-in für SQL Server-Ordner aus dem DR-Backup.

Verwandte Informationen

Video ansehen "Disaster Recovery-APIs" .

Storage Disaster Recovery (DR) für SnapCenter Plug-in für SQL Server

Sie können das SnapCenter Plug-in für SQL Server Storage wiederherstellen, indem Sie den DR-Modus für Storage auf der Seite Globale Einstellungen aktivieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass sich die Plug-ins im Wartungsmodus befinden.
- SnapMirror/SnapVault wird nicht mehr verwendet. "SnapMirror Beziehungen unterbrechen"
- Verbinden Sie die LUN aus dem sekundären Server mit dem gleichen Laufwerksbuchstaben.
- Stellen Sie sicher, dass alle Laufwerke mit denselben Laufwerksbuchstaben verbunden sind, die vor der DR verwendet wurden.
- MSSQL-Serverdienst neu starten.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

Über diese Aufgabe

Disaster Recovery (DR) wird auf VMDK- und RDM-Konfigurationen nicht unterstützt.

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **Disaster Recovery**.
2. Wählen Sie **Disaster Recovery Aktivieren**.
3. Klicken Sie Auf **Anwenden**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Monitor** > **Jobs** klicken.

Nachdem Sie fertig sind

- Falls neue Datenbanken nach dem Failover erstellt werden, befinden sich die Datenbanken außerhalb des DR-Modus.

  Die neuen Datenbanken laufen weiterhin so wie vor dem Failover.

- Die neuen Backups, die im DR-Modus erstellt wurden, werden auf der Topologieseite unter SnapMirror oder SnapVault (sekundär) aufgeführt.

  Neben den neuen Backups wird ein „i“-Symbol angezeigt, das angibt, dass diese Backups während des DR-Modus erstellt wurden.

- Sie können das SnapCenter-Plug-in für SQL Server-Backups löschen, das während des Failovers erstellt wurde, entweder mit der Benutzeroberfläche oder mit dem folgenden Cmdlet: `Remove-SmBackup`
- Wenn sich einige Ressourcen nach dem Failover im nicht-DR-Modus befinden sollen, verwenden Sie das folgende Cmdlet: `Remove-SmResourceDRMode`

  Weitere Informationen finden Sie im "SnapCenter Software Cmdlet Referenzhandbuch".

- SnapCenter Server verwaltet die einzelnen Storage-Ressourcen (SQL-Datenbanken) im DR- oder nicht-DR-Modus, jedoch nicht die Ressourcengruppe mit Storage-Ressourcen, die sich im DR-Modus oder nicht im DR-Modus befinden.

Failback von sekundärem SnapCenter Plug-in für SQL Server Storage auf den Primärspeicher

Nachdem das SnapCenter Plug-in für den primären SQL Server Storage wieder online ist, sollten Sie ein Failback auf den primären Storage durchführen.

Bevor Sie beginnen

- Setzen Sie das SnapCenter-Plug-in für SQL Server auf der Seite Managed Hosts in den **Maintenance** -Modus.
- Trennen Sie den sekundären Speicher vom Host, und stellen Sie eine Verbindung zum primären Speicher her.
- Für ein Failback auf den primären Storage stellen Sie sicher, dass die Beziehungsrichtung vor dem Failover unverändert bleibt, indem Sie den umgekehrten Resync-Vorgang durchführen.

  Um die Rollen des primären und sekundären Storage nach der umgekehrten Resync-Operation beizubehalten, führen Sie die erneute Umkehr-Resynchronisierung erneut durch.

  Weitere Informationen finden Sie unter "Spiegelbeziehungen neu synchronisieren"

- MSSQL-Serverdienst neu starten.
- Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.

> Beim Failover oder Failback des Plug-ins wird der Gesamtstatus des Plug-ins nicht sofort aktualisiert. Der Gesamtstatus von Host und Plug-in wird während der nachfolgenden Aktualisierung des Hosts aktualisiert.

Schritte

1. Navigieren Sie auf der Seite Einstellungen zu **Einstellungen** > **Globale Einstellungen** > **Disaster Recovery**.
2. Deaktivieren Sie Die Option * Disaster Recovery Aktivieren*.
3. Klicken Sie Auf **Anwenden**.
4. Überprüfen Sie, ob der DR-Job aktiviert ist oder nicht, indem Sie auf **Monitor** > **Jobs** klicken.

Nachdem Sie fertig sind

Sie können das SnapCenter-Plug-in für SQL Server-Backups löschen, das während des Failovers erstellt wurde, entweder mit der Benutzeroberfläche oder mit dem folgenden Cmdlet: `Remove-SmDRFailoverBackups`

Installieren Sie das SnapCenter Plug-in für VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

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

Konfigurieren Sie die CRL-Datei

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

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

Bereiten Sie sich auf die Datensicherung 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.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich bei SnapCenter an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen oder zuweisen und Anmeldedaten erstellen.

  SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss über einen eindeutigen Namen verfügen.

- Fügen Sie Hosts hinzu, installieren Sie die Plug-ins, ermitteln 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 mit Invoke-SmConfigureResources.

  Informationen zum Ausführen des Cmdlet finden Sie im "SnapCenter Software Cmdlet Referenzhandbuch"

- Wenn Sie SnapCenter Server zum Schutz von SQL Datenbanken nutzen, die sich auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren. Die Dokumentation zum SnapCenter Plug-in für VMware vSphere enthält weitere Informationen.

  "Dokumentation zum SnapCenter Plug-in für VMware vSphere"

- Führen Sie die Host-seitige Storage-Bereitstellung mit dem SnapCenter Plug-in für Microsoft Windows durch.
- Richten Sie SnapMirror- und SnapVault-Beziehungen ein, falls Sie eine Backup-Replizierung möchten.

Weitere Informationen finden Sie unter SnapCenter Installationsinformationen.

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für SnapCenter 4.3.x-Anwender enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Filesysteme mithilfe des Linux-basierten SnapCenter Plug-ins für VMware vSphere Virtual Appliance (Open Virtual Appliance Format).

"Dokumentation zum SnapCenter Plug-in für VMware vSphere"

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SQL Server verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind typischerweise 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 von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

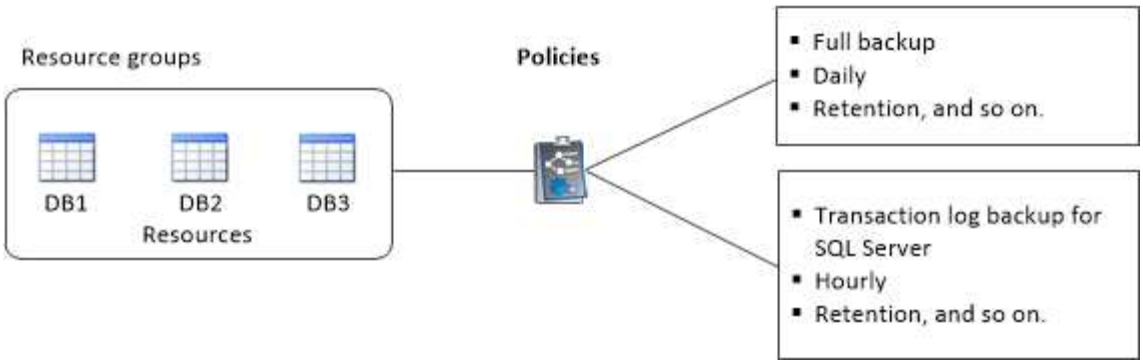
  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, die Aufbewahrung von Kopien, die Replizierung, Skripte und andere Merkmale von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme des Hosts enthält. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass sie täglich ein vollständiges Backup durchführt, und einen anderen Zeitplan, der stündlich Protokoll-Backups durchführt.

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



Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe

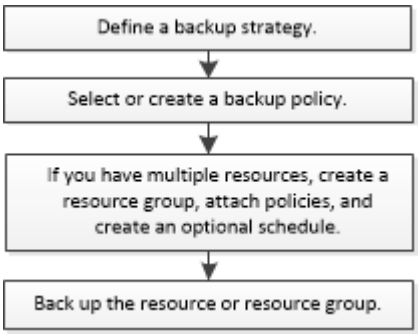
Backup-Workflow

Wenn Sie das SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung installieren, können Sie mit SnapCenter die SQL Server Ressourcen sichern.

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden.

Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden.

Der folgende Workflow zeigt die Reihenfolge, in der Sie die Backup-Vorgänge durchführen müssen:



Die Optionen „Jetzt sichern“, „Wiederherstellen“, „Backups verwalten“ und „Klonen“ auf der Seite „Ressourcen“ werden deaktiviert, wenn Sie eine nicht von NetApp stammende LUN, eine beschädigte Datenbank oder eine wiederhergestellte Datenbank auswählen.

Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch"

Wie SnapCenter Datenbanken sichert

SnapCenter verwendet Snapshot Technologie, um die SQL Server Datenbanken auf LUNs oder VMDKs zu sichern. SnapCenter erstellt das Backup durch Erstellen von Snapshots der Datenbanken.

Wenn Sie auf der Seite Ressourcen eine Datenbank für ein vollständiges Datenbank-Backup auswählen, wählt SnapCenter automatisch alle anderen Datenbanken aus, die sich auf demselben Storage Volume 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 neu auswählen.

Alle Datenbanken, die sich auf einem einzelnen Volume befinden, werden gleichzeitig mithilfe von Snapshots gesichert. Wenn die maximale Anzahl gleichzeitiger Backup-Datenbanken 35 ist und sich mehr als 35 Datenbanken auf einem Speicher-Volume befinden, dann entspricht die Gesamtzahl der erstellten Snapshots der Anzahl der Datenbanken geteilt durch 35.

Sie können die maximale Anzahl an Datenbanken für jeden Snapshot in der Backup-Richtlinie konfigurieren.

Wenn SnapCenter einen Snapshot erstellt, wird im Snapshot das gesamte Storage-System-Volume erfasst. Das Backup ist jedoch nur für den SQL-Hostserver gültig, für den das Backup erstellt wurde.

Wenn sich Daten von anderen SQL Host-Servern auf demselben Volume befinden, können diese Daten vom Snapshot nicht wiederhergestellt werden.

Weitere Informationen

"Fehler beim Quiesce oder Gruppieren von Ressourcen"

Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind

Ressourcen sind die Datenbanken, Applikationsinstanzen, Verfügbarkeitsgruppen und ähnliche Komponenten, die von den installierten Plug-ins gewartet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsjobs ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie zur Verfügung haben. Das ermitteln der verfügbaren Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen.
- Um die Microsoft SQL-Datenbanken zu ermitteln, sollte 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 oben genannte 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 der Benutzer kann ein SQL- oder Windows-Benutzer sein.
- Um die Microsoft SQL-Datenbanken in einem Windows-Cluster zu ermitteln, müssen Sie den TCP/IP-Port (Failover Cluster Instance) für die Failover-Cluster-Instanz (FCI) freigeben.
- Wenn Datenbanken auf VMware RDM-LUNs oder VMDKs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Implementieren Sie das SnapCenter Plug-in für VMware vSphere"
- Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und System Admin-Berechtigungen

verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

Über diese Aufgabe

Datenbanken können nicht gesichert werden, wenn die Option **Gesamtstatus** auf der Seite Details auf nicht verfügbar für Backups eingestellt ist. Die Option **Gesamtstatus** ist für die Sicherung auf nicht verfügbar eingestellt, wenn eine der folgenden Optionen zutrifft:

- Datenbanken sind nicht auf einer NetApp LUN.
- Datenbanken befinden sich nicht im normalen Zustand.

  Datenbanken befinden sich nicht im normalen Zustand, wenn sie offline sind, sie wiederherstellen, ausstehende Wiederherstellung, Verdacht usw.

- Datenbanken verfügen über unzureichende Berechtigungen.

  Wenn ein Benutzer beispielsweise nur Zugriff auf die Datenbank hat, können Dateien und Eigenschaften der Datenbank nicht identifiziert werden und können daher nicht gesichert werden.

SnapCenter kann nur die primäre Datenbank sichern, wenn Sie eine Verfügbarkeitsgruppe auf der SQL Server Standard Edition 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 auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** * oder **Instanz** oder **Verfügbarkeitsgruppe** aus.

   Klicken Sie auf , und wählen Sie den Hostnamen und die SQL Server-Instanz aus, um die Ressourcen zu filtern. Sie können dann klicken , um den Filterbereich zu schließen.

3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden in den SnapCenter-Serverbestand aktualisiert.

   Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Host- oder Cluster-Name, zugeordnete Ressourcengruppen, Backup-Typ, 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 Datensicherungsvorgänge für eine Datenbank ausführen, die sich auf einem Storage-System anderer Anbieter befindet.

   - Wenn sich die Datenbank auf einem NetApp-Speicher befindet und nicht geschützt ist, `Not protected` wird in der Spalte **Gesamtstatus** angezeigt.
   - Wenn sich die Datenbank auf einem NetApp-Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche `Backup not run` eine Meldung in der Spalte **Gesamtstatus** an.

◦ Wenn sich die Datenbank auf einem NetApp-Speichersystem befindet und geschützt ist und das Backup für die Datenbank ausgelöst wird, wird auf der Benutzeroberfläche die Meldung in der Spalte **Gesamtstatus** angezeigt `Backup succeeded`.

Wenn Sie beim Einrichten der Anmeldeinformationen eine SQL-Authentifizierung aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Vorhängeschloss-Symbol angezeigt. Wenn das Vorhängeschloss-Symbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, damit die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzugefügt werden kann.

1. Nachdem der SnapCenter-Administrator einem RBAC-Benutzer die Ressourcen zuweist, muss sich der RBAC-Benutzer anmelden und auf **Ressourcen aktualisieren** klicken, um die neuesten **Gesamtstatus** der Ressourcen anzuzeigen.

Migrieren von Ressourcen auf ein NetApp Storage-System

Nachdem Sie Ihr NetApp Storage-System mit dem SnapCenter Plug-in für Microsoft Windows bereitgestellt haben, können Sie Ihre Ressourcen auf das NetApp Storage-System oder von einer NetApp LUN zu einer anderen NetApp LUN migrieren. Hierzu stehen entweder die SnapCenter Graphical User Interface (GUI) oder die PowerShell Commandlets zur Verfügung.

Bevor Sie beginnen

- Sie müssen dem SnapCenter-Server Storage-Systeme hinzugefügt haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. In den folgenden Informationen werden einige der Felder beschrieben, für die Sie möglicherweise eine Anleitung 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 in der Dropdown-Liste **Ansicht** 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 durch:

Für dieses Feld…	Tun Sie das…
Datenbankname (optional)	Wenn Sie eine Instanz für die Migration ausgewählt haben, müssen Sie die Datenbanken dieser Instanz aus der Dropdown-Liste **Databases** auswählen.

Für dieses Feld…	Tun Sie das…
Wählen Sie Reiseziele	Wählen Sie den Zielspeicherort für Daten- und Protokolldateien aus. Die Daten- und Log-Dateien werden in den Daten- bzw. Log-Ordner unter dem ausgewählten NetApp-Laufwerk verschoben. Wenn kein Ordner in der Ordnerstruktur vorhanden ist, wird ein Ordner erstellt und die Ressource migriert.
Details zur Datenbankdatei anzeigen (optional)	Wählen Sie diese Option aus, wenn Sie mehrere Dateien einer einzigen Datenbank migrieren möchten. Diese Option wird nicht angezeigt, wenn Sie die Ressource **Instanz** auswählen.
Optionen	Wählen Sie **Kopie der migrierten Datenbank am ursprünglichen Speicherort löschen**, um die Kopie der Datenbank aus der Quelle zu löschen. Optional: **UPDATE-STATISTIKEN auf Tabellen AUSFÜHREN, bevor Sie die Datenbank entfernen**.

5. Führen Sie auf der Seite Verifizieren die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Optionen Zur Datenbankkonsistenzprüfung	Wählen Sie **vorher ausführen** aus, um die Integrität der Datenbank vor der Migration zu überprüfen. Wählen Sie **nach** ausführen, um die Integrität der Datenbank nach der Migration zu überprüfen.

Für dieses Feld…	Tun Sie das…
DBCC CHECKDB Optionen	• Wählen Sie die Option **PHYSICAL_ONLY**, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um zerrissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen. • Wählen Sie die Option **NO_INFOMSGS**, um alle Informationsmeldungen zu unterdrücken. • Wählen Sie die Option **ALL_ERRORMSGS** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen. • Wählen Sie die Option **NOINDEX** aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten. Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen. Sie können diese Option auswählen, um die Ausführungszeit zu verkürzen. • Wählen Sie die Option **TABLOCK**, um die Prüfungen zu beschränken und Sperren anstelle eines internen Datenbank-Snapshots zu erhalten.

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

Erstellen von Backup-Richtlinien 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. Alternativ können Sie beim Erstellen einer Ressourcengruppen oder beim Sichern einer einzelnen Ressource eine Backup-Richtlinie erstellen.

Bevor Sie beginnen

- Sie müssen Ihre Datensicherungsstrategie definiert haben.
- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Storage-System abschließen.
- Sie müssen das Host-Protokollverzeichnis für die Protokollsicherung konfiguriert haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss der SnapCenter Administrator Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.

  Informationen darüber, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den SnapCenter Installationsinformationen.

- 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.

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

Über diese Aufgabe

- Eine Backup-Richtlinie ist eine Reihe von Regeln, die festlegen, wie Backups gemanagt und aufbewahrt werden und wie oft die Ressourcen- oder Ressourcengruppe gesichert wird. Außerdem können Sie Replizierungs- und Skript-Einstellungen festlegen. Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.

  DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

- SnapLock

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

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

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

  Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritt: Richtliniennamen Erstellen

1. Wählen Sie im linken Navigationsbereich **Einstellungen**.
2. Wählen Sie auf der Seite Einstellungen die Option **Richtlinien** aus.
3. Wählen Sie **Neu**.

4. Geben Sie auf der Seite **Name** den Namen und die Beschreibung der Richtlinie ein.

Schritt 2: Konfigurieren von Backup-Optionen

1. Wählen Sie Ihren Sicherungstyp aus

Vollständige Sicherung und Protokollsicherung

Sichern Sie die Datenbankdateien und Transaktionsprotokolle und verkürzen Sie die Transaktionsprotokolle.

1. Wählen Sie **Vollbackup und Log Backup** aus.
2. Geben Sie die maximale Anzahl an Datenbanken ein, die für jeden Snapshot gesichert werden sollen.

> Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.

Vollständiges Backup

Sichern Sie die Datenbankdateien.

1. Wählen Sie * Vollbackup* aus.
2. Geben Sie die maximale Anzahl an Datenbanken ein, die für jeden Snapshot gesichert werden sollen. Der Standardwert ist 100

> Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.

Backup Protokollieren

1. Sichern Sie die Transaktionsprotokolle.
2. Wählen Sie **Backup protokollieren**.

Backup Nur Kopieren

1. Wenn Sie Ihre Ressourcen mithilfe einer anderen Backup-Anwendung sichern, wählen Sie **nur Backup kopieren**.

Wenn die Transaktionsprotokolle intakt bleiben, kann jede Backup-Anwendung die Datenbanken wiederherstellen. In der Regel sollten Sie die Option nur kopieren unter anderen Umständen nicht verwenden.

> Microsoft SQL unterstützt nicht die Option **nur kopieren Backup** zusammen mit der Option **Vollbackup und Log Backup** für sekundären Speicher.

1. Führen Sie im Abschnitt Einstellungen für Verfügbarkeitsgruppen die folgenden Aktionen durch:

   a. Nur Backup auf bevorzugtem Backup-Replikat.

      Wählen Sie diese Option aus, um nur auf dem bevorzugten Backup-Replikat zu sichern. Über die für die AG im SQL Server konfigurierten Backup-Einstellungen wird das bevorzugte Backup-Replikat entschieden.

b. Wählen Sie Replikate für das Backup aus.

   Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für das Backup aus.

c. Backup-Priorität auswählen (minimale und maximale Backup-Priorität)

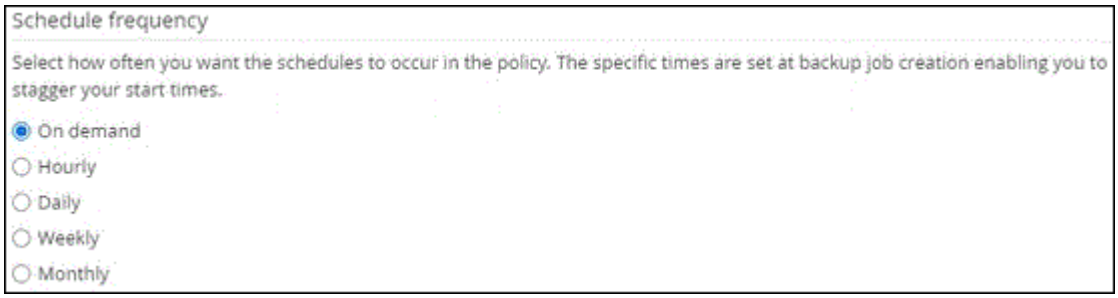
   Geben Sie eine Mindestanzahl der Backup-Prioritäten und eine Nummer der maximalen Backup-Priorität an, die das AG-Replikat für das Backup entscheidet. Sie können beispielsweise eine Mindestpriorität von 10 und eine maximale Priorität von 50 haben. In diesem Fall werden alle AG-Replikate mit einer Priorität von mehr als 10 und weniger als 50 für Backups in Betracht gezogen.

   Standardmäßig ist die Mindestpriorität 1 und die maximale Priorität 100.

Bei Cluster-Konfigurationen werden die Backups entsprechend den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Node des Clusters aufbewahrt. Wenn sich der Owner-Knoten der AG ändert, werden die Backups gemäß den Aufbewahrungseinstellungen erstellt und die Backups des vorherigen Owner-Knotens beibehalten. Die Aufbewahrung für AG ist nur auf Node-Ebene anwendbar.

2. Planen Sie die Backup-Häufigkeit für diese Richtlinie. Geben Sie den Zeitplantyp an, indem Sie entweder **On Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

   Sie können nur einen Plantyp für eine Richtlinie auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang festlegen, während Sie eine Ressourcengruppe erstellen. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

Schritt 3: Konfigurieren der Aufbewahrungseinstellungen

Führen Sie auf der Seite Aufbewahrung je nach dem auf der Seite Backup-Typ ausgewählten Backup-Typ eine oder mehrere der folgenden Aktionen durch:

1. Führen Sie in den Aufbewahrungseinstellungen für den Abschnitt „minutengenaue Wiederherstellung“ eine der folgenden Aktionen aus:

Bestimmte Anzahl von Kopien

Bewahren Sie nur eine bestimmte Anzahl von Snapshots auf.

1. Wählen Sie die Option **Protokoll-Backups aufbewahren, die für die letzte <Zahl> Tage** gelten, und geben Sie die Anzahl der zu beheldenden Tage an. Wenn Sie diesem Limit nahe kommen, können Sie ältere Kopien löschen.

Bestimmte Anzahl von Tagen

Bewahren Sie die Backup-Kopien für eine bestimmte Anzahl von Tagen auf.

1. Wählen Sie die Option **Protokoll-Backups aufbewahren, die für die letzten <number> Tage voller Backups** gelten, und geben Sie die Anzahl der Tage an, um die Backup-Kopien des Protokolls zu behalten.

1. Führen Sie im Abschnitt **vollständige Backup-Aufbewahrungs-Einstellungen** für die Einstellungen für On Demand-Aufbewahrung die folgenden Aktionen aus:
   a. Geben Sie die Gesamtzahl der zu erbehalt enden Snapshots an
      i. Um die Anzahl der zu befolgenden Snapshots anzugeben, wählen Sie **Gesamtanzahl der zu befolgenden Snapshot-Kopien** aus.
      ii. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht.

Standardmäßig ist der Wert der Aufbewahrungsanzahl auf 2 festgelegt. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.

1. Dauer der Aufbewahrung von Snapshots
   a. Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshots vor dem Löschen behalten möchten, wählen Sie **Snapshot-Kopien beibehalten für**.
2. Wenn Sie die Sperrfrist für Snapshots angeben möchten, wählen Sie **Sperrfrist für Snapshot-Kopie** und wählen Sie Tage, Monate oder Jahre aus.

   Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

3. Geben Sie im Abschnitt **vollständige Backup-Aufbewahrungseinstellungen** für die Einstellungen für die stündliche, tägliche, wöchentliche und monatliche Aufbewahrung die Aufbewahrungseinstellungen für den Terminplantyp an, der auf der Seite Backup-Typ ausgewählt wurde.
   a. Geben Sie die Gesamtzahl der zu erbehalt enden Snapshots an
      i. Um die Anzahl der zu befolgenden Snapshots anzugeben, wählen Sie **Gesamtanzahl der zu befolgenden Snapshot-Kopien** aus. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht.

Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

1. Dauer der Aufbewahrung von Snapshots
   a. Um die Anzahl der Tage anzugeben, für die Sie die Snapshots vor dem Löschen behalten möchten, wählen Sie **Snapshot Kopien beibehalten für**.
2. Wenn Sie die Sperrfrist für Snapshots angeben möchten, wählen Sie **Sperrfrist für Snapshot-Kopie** und wählen Sie Tage, Monate oder Jahre aus.

   Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

   Die Snapshot-Protokollaufbewahrung ist standardmäßig auf 7 Tage eingestellt. Verwenden Sie das Cmdlet "Set-SmPolicy", um die Snapshot Aufbewahrung des Protokolls zu ändern.

Dieses Beispiel setzt die Snapshot-Protokollaufbewahrung auf 2:

Beispiel 1. Beispiel Anzeigen

```
Set-SmPolicy -PolicyName 'newpol' -PolicyTyp 'Backup' -PluginPolicyTyp 'SCSQL' -sqlbackuptyp
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='hourly';RetentionCount=2},@{2}@{2}
BackupType='LOG';ScheduleType='hourly'
```

"SnapCenter behält Snapshot Kopien der Datenbank bei"

Schritt 4: Konfigurieren der Replikationseinstellungen

1. Geben Sie auf der Seite „Replikation“ die Replikation auf das sekundäre Speichersystem an:

SnapMirror aktualisieren

Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie.

1. Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu erstellen.

   Diese Option sollte für SnapMirror Active Sync aktiviert sein.

   Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden.

   Siehe "Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an".

Aktualisieren Sie SnapVault

Aktualisieren Sie SnapVault nach dem Erstellen einer Snapshot Kopie.

1. Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.

   Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden.

   Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert.

   Weitere Informationen zu SnapLock Vault finden Sie unter "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel"

   Siehe "Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an".

Sekundäre Richtlinienbezeichnung

1. Wählen Sie eine Snapshot-Bezeichnung aus.

Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht.

> Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.

Fehler Anzahl Der Wiederholungen

1. Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

Schritt 5: Konfigurieren der Skripteinstellungen

1. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Backup ausgeführt werden sollen.

Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren und Protokolle zu senden.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

Sie müssen die SnapMirror Aufbewahrungsrichtlinie in ONTAP so konfigurieren, dass der sekundäre Storage nicht die maximale Snapshot-Grenze erreicht.

Schritt 6: Konfigurieren Sie die Überprüfungseinstellungen

Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

1. Wählen Sie im Abschnitt Überprüfung ausführen für folgende Backup-Pläne die Zeitplanhäufigkeit aus.
2. Führen Sie im Abschnitt Optionen für die Datenbankkonsistenzprüfung die folgenden Aktionen durch:
   a. Beschränkung der Integritätsstruktur auf die physische Struktur der Datenbank (PHYSICAL_ONLY)
      i. Wählen Sie **Beschränkung der Integritätsstruktur auf physische Struktur der Datenbank (PHYSICAL_ONLY)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um gerissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen.
   b. Alle Informationsmeldungen unterdrücken (KEINE INFOMSGS)
      i. Wählen Sie * Alle Informationsmeldungen (NO_INFOMSGS)* aus, 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)** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen.
   d. Nicht geclusterte Indizes (NOINDEX) nicht prüfen
      i. Wählen Sie * nicht gruppierte Indizes (NOINDEX)* aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten. Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.
   e. Begrenzen Sie die Überprüfungen und erhalten Sie die Sperren anstelle eines internen Datenbank-Snapshot (TABLOCK)
      i. Wählen Sie **Schränken Sie die Prüfungen ein und erhalten Sie die Sperren anstatt eine interne Datenbank Snapshot Kopie (TABLOCK)** zu verwenden, um die Überprüfungen zu begrenzen und Sperren anstelle eines internen Datenbank-Snapshots zu erhalten.
3. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss bestätigen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
4. Geben Sie im Abschnitt **Verification Script settings** den Pfad und die Argumente des Vorskripts bzw. Postscript ein, die vor oder nach dem Verifizierungsvorgang ausgeführt werden sollen.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

Schritt 7: Zusammenfassung überprüfen

1. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server

Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie gemeinsam sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Sie können Ressourcen einzeln schützen, ohne eine neue Ressourcengruppe zu erstellen. Sie können Backups auf der geschützten Ressource erstellen.

Über diese Aufgabe

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

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

Für dieses Feld…	Tun Sie das…
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird an den 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 Dropdown-Listen aus, um die Liste der Ressourcen zu filtern.

      Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

   b. So verschieben Sie Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** in den Abschnitt Ausgewählte Ressourcen:
      - Wählen Sie **Automatische Auswahl aller Ressourcen auf demselben Speichervolumen**, 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 Pfeil nach rechts, 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 Dropdown-Liste aus.

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

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

   b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies auf * * in der Spalte Configure Schedules für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
   c. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **OK** klicken.

      Sie müssen dies für jede in der Richtlinie angegebene Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte angewendete Zeitpläne im Abschnitt **Zeitpläne für ausgewählte Richtlinien konfigurieren** aufgelistet.

d. Wählen Sie den Microsoft SQL Server Scheduler aus.

   Sie müssen auch eine Planer-Instanz auswählen, die der Planungsrichtlinie zugeordnet werden soll.

   Wenn Sie den Microsoft SQL Server Scheduler nicht auswählen, ist der Standard Microsoft Windows Scheduler.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden. Sie sollten die Zeitpläne nicht ändern und den Backupjob umbenennen, der in Windows Scheduler oder SQL Server Agent erstellt wurde.

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

   a. Wählen Sie den Verifikationsserver aus der Dropdown-Liste **Überprüfungsserver** aus.

      Die Liste enthält alle SQL Server, die in SnapCenter hinzugefügt wurden. Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).

      Die Version des Verifizierungsservers sollte mit der Version und Edition des SQL-Servers übereinstimmen, der die primäre Datenbank hostet.

   a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror und SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf * * + .
   c. Führen Sie im Dialogfeld Add Verification Schedules Policy_Name die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen**.

   d. Klicken Sie auf **OK**.

      Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt. Sie können die Informationen überprüfen und dann bearbeiten, indem Sie auf * * *  klicken oder durch Klicken auf * * * löschen ✖ .

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

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

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

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

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

Anforderungen für das Backup 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 Storage-System in ein NetApp Storage-System migriert haben.
- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung zu einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Der von einem Active Directory (AD)-Benutzer initiierte Backup-Vorgang schlägt fehl, wenn die SQL-Instanz-Anmeldeinformationen nicht dem AD-Benutzer oder der AD-Gruppe zugewiesen sind. Sie müssen die SQL-Instanz-Anmeldeinformationen AD-Benutzer oder -Gruppe über die Seite **Einstellungen** > **Benutzerzugriff** zuweisen.
- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts enthält, kann der Backup-Vorgang auf einigen Hosts aufgrund von Netzwerkproblemen spät ausgelöst werden. Sie sollten den Wert von FMaxRetryForUninitializedHosts in Web.config mit dem Cmdlet Set-SmConfigSettings PS konfigurieren.

Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um Datensicherungsvorgänge durchzuführen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und

eine eindeutige Management-LIF-IP-Adresse verfügen.

Schritte

1. Starten Sie eine PowerShell Core-Verbindungssitzung mit dem Cmdlet "Open-SmConnection".

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

   ```
   PS C:\> Open-SmConnection
   ```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

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

Backup von SQL-Ressourcen

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

Über diese Aufgabe

- Für die Authentifizierung von Windows-Anmeldeinformationen müssen Sie die 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 beim Registrieren des Hosts mit SnapCenter auf der Seite **Add Host** oder **Modify Host** einrichten, um den gMSA zu aktivieren und zu verwenden.
- Wenn der Host mit gMSA hinzugefügt wird und das gMSA über Login- und Systemadministratorrechte verfügt, darf gMSA eine Verbindung zur SQL-Instanz herstellen.
  - SnapCenter überprüft, ob die Authentifizierung für SQL-Instanzen konfiguriert ist. Wenn die Authentifizierung konfiguriert ist, wird über diese Anmeldeinformationen auf die SQL-Instanz zugegriffen.

- Wenn die Authentifizierung nicht konfiguriert ist, verwenden Sie gMSA, um zu prüfen, ob das SQL-Plug-in derzeit funktioniert. Wenn das Plug-in funktioniert, wird es verwendet, um eine Verbindung zur SQL-Instanz herzustellen.
- Der Zugriff auf die SQL-Instanz erfolgt über die Windows-Anmeldeinformationen-Authentifizierung, wenn die Authentifizierung für SQL-Instanzen nicht konfiguriert ist und das Plug-in nicht betriebsbereit ist.

UI von SnapCenter

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen * Datenbank* oder **Instanz** oder **Verfügbarkeitsgruppe** aus der Dropdown-Liste **Ansicht** aus.

   a. Wählen Sie die Datenbank, die Instanz oder die Verfügbarkeitsgruppe aus, die Sie sichern möchten.

      Wenn Sie eine Sicherungskopie einer Instanz erstellen, sind die Informationen zum letzten Sicherungsstatus oder zum Zeitstempel dieser Instanz auf der Seite Ressourcen nicht verfügbar.

   In der Topologieansicht lässt sich nicht unterscheiden, ob der Backup-Status, der Zeitstempel oder das Backup für eine Instanz oder eine Datenbank gilt.

3. Aktivieren Sie auf der Seite „Ressourcen“ das Kontrollkästchen **benutzerdefiniertes Namensformat für Snapshot-Kopie**, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

   Beispiel: Custtext_Policy_hostname oder Resource_hostname. Standardmäßig wird an den 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 Dropdown-Liste aus.

      Sie können eine Richtlinie erstellen, indem Sie * * auswählen  , um den Richtlinien-Assistenten zu starten.

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

   b. Wählen Sie * *  in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld **Add Schedules for Policy** `policy_name` den Zeitplan und wählen Sie dann **OK** aus.

      Hier `policy_name` ist der Name der Richtlinie, die Sie ausgewählt haben.

   Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

   a. Wählen Sie den Microsoft SQL Server Scheduler verwenden* aus, und wählen Sie dann die Planerinstanz aus der Dropdown-Liste **Scheduler Instance** aus, die mit der Planungsrichtlinie verknüpft ist.

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

   a. Wählen Sie den Verifikationsserver aus der Dropdown-Liste **Überprüfungsserver** 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, der die primäre Datenbank hostet.

a. Wählen Sie **sekundäre Lokatoren 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 Überprüfungsplan konfigurieren möchten, und wählen Sie dann * * aus.

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

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen**.

Wenn der Verifikationsserver keine Speicherverbindung hat, schlägt der Verifizierungsvorgang mit Fehler fehl: Datenträger konnte nicht bereitgestellt werden.

d. Wählen Sie **OK**.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

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

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

7. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Die Seite der Datenbanktopologie wird angezeigt.

8. Wählen Sie **Jetzt sichern**.

9. Führen Sie auf der Seite Backup die folgenden Schritte aus:

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

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

b. Wählen Sie zur Überprüfung Ihres Backups **nach dem Backup**.

c. Wählen Sie **Backup**.

> Sie sollten den im Windows Scheduler oder SQL Server Agent erstellten Sicherungsauftrag nicht umbenennen.

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

Es wird eine implizite Ressourcengruppe erstellt. Sie können dies anzeigen, indem Sie auf der Seite „Benutzerzugriff“ den jeweiligen Benutzer oder die jeweilige Gruppe auswählen. Der implizite Gruppentyp lautet „`Ressource`“.

10. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Nachdem Sie fertig sind

- In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen. Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei /opt/netapp/init_scvservice. In diesem Skript startet der `do_start method` Befehl den SnapCenter VMware Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

"Backup-Vorgänge schlagen wegen der Verzögerung im TCP_TIMEOUT bei MySQL-Verbindungsfehler fehl"

"Das Backup schlägt mit dem Windows Scheduler-Fehler fehl"

"Fehler beim Quiesce oder Gruppieren von Ressourcen"

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem SQL Backup-Typ von FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

In diesem Beispiel wird eine neue Backup-Richtlinie mit einem Backup-Typ von CrashConsistent für Windows File-Systeme erstellt:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Ermitteln Sie Host-Ressourcen mit dem Cmdlet "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
```

   In diesem Beispiel werden Ressourcen für Windows File-Systeme auf dem angegebenen Host ermittelt:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Fügen Sie mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter hinzu.

   In diesem Beispiel wird eine neue Ressourcengruppe für die Sicherung von SQL-Datenbanken 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"
```

   Dieses Beispiel erstellt eine neue Windows Dateisystem-Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

   In diesem Beispiel wird ein Job-Summary-Bericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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

Sichern Sie SQL Server-Ressourcengruppen

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie * *auswählen und dann das Tag auswählen. Sie können dann * * auswählen, um das Filterfenster 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

   b. Wählen Sie nach dem Backup **Verify** aus, um das On-Demand-Backup zu überprüfen.

      Die Option **Verify** in der Richtlinie gilt nur für geplante Jobs.

   c. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

"Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server"

"Backup-Vorgänge schlagen wegen der Verzögerung im TCP_TIMEOUT bei MySQL-Verbindungsfehler fehl"

"Das Backup schlägt mit dem Windows Scheduler-Fehler fehl"

Überwachen Sie die Backup-Vorgänge für SQL-Ressourcen auf der Seite SnapCenter-Jobs

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

Überwachen Sie Datenschutzvorgänge für SQL-Ressourcen im Bereich „Aktivität“

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

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

Schritte

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

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

Abbrechen des SnapCenter-Plug-ins für Microsoft SQL Server-Backup-Vorgänge

Sie können laufende, in die Warteschlange eingereihte oder nicht reaktionsfähige Backup-Vorgänge abbrechen. Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter-Server den Vorgang und entfernt alle Snapshots aus dem Speicher, wenn das erstellte Backup nicht beim SnapCenter-Server registriert ist. Wenn das Backup bereits beim SnapCenter-Server registriert ist, wird ein Rollback des bereits erstellten Snapshots selbst dann nicht durchgeführt, wenn der Abbruch ausgelöst wurde.

Bevor Sie beginnen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.
- Sie können nur das Protokoll oder die vollständigen Backup-Vorgänge abbrechen, die in die Warteschlange gestellt werden oder ausgeführt werden.
- Sie können den Vorgang nicht abbrechen, nachdem die Überprüfung gestartet wurde.

  Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Verifizierungsvorgang wird nicht durchgeführt.

- Sie können einen Sicherungsvorgang entweder über die Seite Überwachen oder über den Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter GUI können Sie PowerShell cmdlets verwenden, um Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Wählen Sie im linken Navigationsbereich **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und wählen Sie **Job abbrechen** .
Aktivitätsbereich	1. Wählen Sie nach dem Starten des Backupjobs im Aktivitätsbereich die Option aus , um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Wählen Sie auf der Seite Job-Details die Option **Job abbrechen** aus.

Ergebnis

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt. Wenn der Vorgang, den Sie abgebrochen haben, im Status Abbrechen oder Ausführen nicht reagiert, sollten Sie das Cmdlet ausführen `Cancel-SmJob -JobID <int> -Force` , um den Sicherungsvorgang gewaltsam anzuhalten.

Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Sie können die folgenden Symbole in der Ansicht **Kopien verwalten** anzeigen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Vault-Kopien).

- Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
- Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.
- Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.
  - Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden.

Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

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

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

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

Schritte

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

   Wenn die ausgewählte Ressource eine geklonte Datenbank ist, schützen Sie die geklonte Datenbank, wird die Quelle des Klons 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. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt **Übersichtskarte** wird die Gesamtzahl der Backups und Klone angezeigt.

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

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

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

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

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

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

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

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

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

7. Wählen Sie einen Klon aus der Tabelle aus und klicken Sie auf **Clone Split**.
8. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf  .

Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets

Sie können das Cmdlet "Remove-SmBackup" verwenden, um die Anzahl der Backups für sekundäre Backups zu bereinigen, die keinen Snapshot haben. Sie können dieses Cmdlet verwenden, wenn die in der Topologie zum Verwalten von Kopien angezeigten Snapshots insgesamt nicht mit der Einstellung für die Aufbewahrung von sekundären SpeicherSnapshot übereinstimmen.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

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

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
   ```

2. Bereinigen Sie die Anzahl der sekundären Backups mit dem Parameter -CleanupSecondaryBackups.

   In diesem Beispiel wird die Anzahl der Backups für sekundäre Backups ohne Snapshots bereinigt:

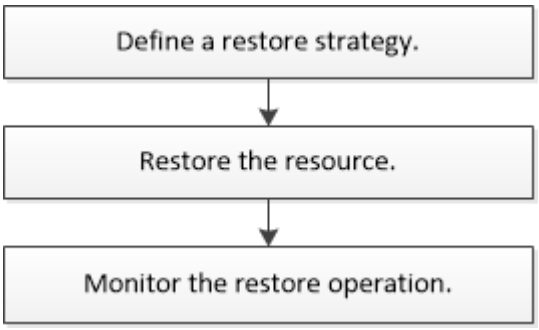
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Stellen Sie SQL Server-Ressourcen wieder her

Wiederherstellung des Workflows

Sie können SnapCenter verwenden, um SQL Server Datenbanken wiederherzustellen, indem Sie die Daten von einem oder mehreren Backups auf Ihr aktives File-System wiederherstellen und dann die Datenbank wiederherstellen. Sie können auch Datenbanken wiederherstellen, die sich in Verfügbarkeitsgruppen befinden, und dann die wiederhergestellten Datenbanken der Verfügbarkeitsgruppe hinzufügen. Vor dem Wiederherstellen einer SQL Server-Datenbank müssen Sie mehrere vorbereitende Aufgaben ausführen.

Im folgenden Workflow wird die Reihenfolge angezeigt, in der Sie die Datenbankwiederherstellungen durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch"

Weitere Informationen

"Wiederherstellung einer SQL Server-Datenbank aus dem sekundären Storage"

"Stellen Sie Ressourcen mithilfe von PowerShell cmdlets wieder her"

"Der Wiederherstellungsvorgang kann unter Windows 2008 R2 fehlschlagen"

Anforderungen für das Wiederherstellen 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 Ziel-SQL Server-Instanz muss online sein und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.

  Dies gilt sowohl für Restore-Vorgänge bei der Benutzerdatenbank als auch für die Wiederherstellung von Systemdatenbanken.

- SnapCenter Vorgänge, die für die wiederherzustellende SQL Server Daten ausgeführt werden, müssen deaktiviert werden, einschließlich sämtlicher Jobs, die auf Remote Management- oder Remote Verifizierungs-Servern geplant sind.
- Wenn Systemdatenbanken nicht funktionsfähig sind, müssen Sie zuerst die Systemdatenbanken mithilfe eines SQL Server-Dienstprogramms neu erstellen.
- Wenn Sie das Plug-in installieren, stellen Sie sicher, dass Sie Berechtigungen für andere Rollen erteilen, um die Backups der Verfügbarkeitsgruppe (AG) wiederherzustellen.

  Die Wiederherstellung der AG schlägt fehl, wenn eine der folgenden Bedingungen erfüllt ist:

  - Wenn das Plug-in durch RBAC-Benutzer installiert wird und ein Administrator versucht, ein AG-Backup wiederherzustellen
  - Wenn das Plug-in von einem Administrator installiert wird und ein RBAC-Benutzer versucht, ein AG-Backup wiederherzustellen
- Wenn Sie benutzerdefinierte Protokollverzeichnis-Backups auf einen alternativen Host wiederherstellen, müssen der SnapCenter Server und der Plug-in-Host dieselbe SnapCenter-Version installiert haben.
- Sie müssen Microsoft Hotfix, KB2887595, installiert haben. Die Microsoft Support Site enthält weitere Informationen über KB2887595.

  "Microsoft Support-Artikel 2887595: Windows RT 8.1, Windows 8.1 und Windows Server 2012 R2 Update Rollup: November 2013"

- Sie müssen die Ressourcengruppen oder die Datenbank gesichert haben.
- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss Ihnen der SnapCenter Administrator die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.

  Informationen darüber, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den SnapCenter Installationsinformationen.

- Alle Backup- und Klonjobs müssen vor der Wiederherstellung der Datenbank angehalten werden.
- Wenn sich die Datenbankgröße in Terabyte (TB) befindet, kann der Restore-Vorgang einen Timeout durchführen.

  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 Zeitüberschreitungswert geändert werden, und der Maximalwert, den Sie einstellen können, beträgt 86400000 ms.

Wenn Sie wiederherstellen möchten, während die Datenbanken online sind, sollte die Option Online-Wiederherstellung auf der Seite Wiederherstellen aktiviert sein.

Stellen Sie Backups von SQL Server Datenbanken wieder her

Sie können SnapCenter verwenden, um gesicherte SQL Server-Datenbanken wiederherzustellen. Die Wiederherstellung der Datenbank ist ein mehrphasiger Prozess, der alle Daten- und Protokollseiten von einem bestimmten SQL Server-Backup in eine angegebene Datenbank kopiert.

Über diese Aufgabe

- Sie können die gesicherten SQL Server Datenbanken auf einer anderen SQL Server-Instanz auf demselben Host wiederherstellen, auf dem das Backup erstellt wurde.

  Sie können SnapCenter verwenden, um die gesicherten SQL Server Datenbanken auf einem anderen Pfad wiederherzustellen, sodass Sie keine Produktionsversion ersetzen.

- SnapCenter kann Datenbanken in einem Windows Cluster wiederherstellen, ohne die SQL Server Cluster-Gruppe offline zu schalten.
- Wenn ein Cluster ausfällt (ein Vorgang zum Verschieben der Cluster-Gruppe) während eines Wiederherstellungsvorgangs auftritt (z. B. wenn der Node, der die Ressourcen besitzt, ausfällt), müssen Sie die Verbindung zur SQL Server Instanz wiederherstellen und dann den Wiederherstellungsvorgang neu starten.
- Sie können die Datenbank nicht wiederherstellen, wenn die Benutzer oder die SQL Server Agent-Jobs auf die Datenbank zugreifen.
- Systemdatenbanken können nicht auf einem alternativen Pfad wiederhergestellt werden.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

- Die meisten Felder auf den Seiten des Assistenten Wiederherstellen sind selbsterklärend. In den folgenden Informationen werden die Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.
- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.
- Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

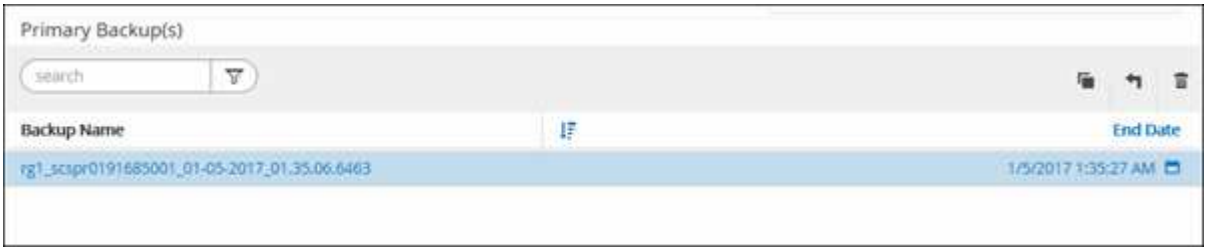
UI von SnapCenter

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.

   Die Topologieseite wird angezeigt.

4. Wählen Sie aus der Ansicht Kopien verwalten im Speichersystem **Backups** aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf das Symbol.



6. Wählen Sie auf der Seite „Bereich wiederherstellen“ eine der folgenden Optionen aus:

Option	Beschreibung
Stellen Sie die Datenbank auf demselben Host wieder her, auf dem das Backup erstellt wurde	Wählen Sie diese Option aus, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Backups erstellt werden.

Option	Beschreibung
Wiederherstellung der Datenbank auf einem alternativen Host	Wählen Sie diese Option aus, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem Backups erstellt werden. Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen ein (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an. Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateiendung der ursprünglichen Datenbankdatei identisch sein. Wenn die Option **Datenbank auf alternativen Host** wiederherstellen nicht auf der Seite „Bereich wiederherstellen“ angezeigt wird, löschen Sie den Browser-Cache.
Stellen Sie die Datenbank mithilfe vorhandener Datenbankdateien wieder her	Wählen Sie diese Option aus, wenn die Datenbank auf einem anderen SQL Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem Backups erstellt werden. Die Datenbankdateien sollten bereits auf den angegebenen Dateipfaden vorhanden sein. Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen ein (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an.

7. Wählen Sie auf der Seite „Recovery Scope“ eine der folgenden Optionen aus:

Option	Beschreibung
Keine	Wählen Sie **Keine** aus, wenn Sie nur das vollständige Backup ohne Protokolle wiederherstellen müssen.
Alle Log-Backups	Wählen Sie **Alle Log-Backups** Backup-Restore-Vorgang up-to-the-minute, um alle verfügbaren Log-Backups nach der vollständigen Sicherung wiederherzustellen.

Option	Beschreibung
Durch Backups bis protokollieren	Wählen Sie **nach Log-Backups**, um einen Point-in-Time-Wiederherstellungsvorgang durchzuführen, der die Datenbank basierend auf Backup-Protokollen bis zum ausgewählten Datum wiederherstellt.
Nach einem bestimmten Datum bis	Wählen Sie **nach einem bestimmten Datum bis**, um Datum und Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht auf die wiederhergestellte Datenbank angewendet werden. Dieser Point-in-Time-Wiederherstellungsvorgang stoppt die Wiederherstellung von Transaktions-Log-Einträgen, die nach dem angegebenen Datum und der angegebenen Zeit aufgezeichnet wurden.
Benutzerdefiniertes Protokollverzeichnis verwenden	Wenn Sie **Alle Log-Backups**, **durch Log-Backups** oder **nach einem bestimmten Datum bis** ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie **Benutzerdefiniertes Log-Verzeichnis verwenden** und geben Sie dann den Speicherort an. Die Option **Benutzerdefiniertes Logverzeichnis verwenden** ist nur verfügbar, wenn Sie **Datenbank auf einen alternativen Host wiederherstellen** oder **Datenbank mit vorhandenen Datenbankdateien wiederherstellen** ausgewählt haben. Sie können auch den freigegebenen Pfad verwenden, aber sicherstellen, dass der SQL-Benutzer auf den Pfad zugreifen kann. Das benutzerdefinierte Protokollverzeichnis wird für die Verfügbarkeitsgruppendatenbank nicht unterstützt.

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 **Überschreiben Sie die Datenbank mit demselben Namen während der Wiederherstellung** aus, um die Datenbank mit dem gleichen Namen wiederherzustellen.
      - Wählen Sie **SQL-Datenbankreplikationseinstellungen beibehalten** aus, um die Datenbank wiederherzustellen und die vorhandenen Replikationseinstellungen beizubehalten.
      - Wählen Sie **Sicherung des Transaktionsprotokolls vor der Wiederherstellung** aus, um ein

Transaktionsprotokoll zu erstellen, bevor der Wiederherstellungsvorgang beginnt.

- Wählen Sie **Wiederherstellen, wenn die Sicherung des Transaktionsprotokolls vor der Wiederherstellung fehlschlägt** aus, um den Wiederherstellungsvorgang abzubrechen, wenn die Sicherung des Transaktionsprotokolls fehlschlägt.

b. Geben Sie optionale Skripte an, die ausgeführt werden sollen, bevor Sie einen Wiederherstellungsauftrag ausführen.

Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares 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 Datenbank nach Abschluss der Wiederherstellung auswählen eine der folgenden Optionen aus:

- Wählen Sie **Operational, aber nicht verfügbar für die Wiederherstellung weiterer Transaktionsprotokolle**, wenn Sie jetzt alle notwendigen Backups wiederherstellen.

  Dies ist das Standardverhalten, das die Datenbank durch ein Rollback der nicht gesicherten Transaktionen einsatzbereit macht. Sie können erst dann weitere Transaktionsprotokolle wiederherstellen, wenn Sie ein Backup erstellen.

- Wählen Sie **nicht betriebsbereit, aber verfügbar für die Wiederherstellung weiterer Transaktionsprotokolle**, um die Datenbank nicht betriebsbereit zu lassen, ohne die nicht gesicherten Transaktionen zurückzurollen.

  Zusätzliche Transaktions-Logs können wiederhergestellt werden. Sie können die Datenbank erst verwenden, wenn sie wiederhergestellt ist.

- Wählen Sie **schreibgeschützter Modus, der zur Wiederherstellung weiterer Transaktionsprotokolle** verfügbar ist, um die Datenbank im schreibgeschützten Modus zu belassen.

  Mit dieser Option werden nicht gesicherte Transaktionen rückgängig gemacht, die nicht rückgängig gemachte Aktionen werden jedoch in einer Standby-Datei gespeichert, sodass Recovery-Effekte rückgängig gemacht werden können.

Wenn die Option „Verzeichnis aufheben“ aktiviert ist, werden mehr Transaktionsprotokolle wiederhergestellt. Wenn der Wiederherstellungsvorgang für das Transaktionsprotokoll nicht erfolgreich ist, können die Änderungen zurückgesetzt werden. Die SQL Server-Dokumentation enthält weitere Informationen.

b. Geben Sie optionale Skripts an, die ausgeführt werden sollen, nachdem ein Wiederherstellungsauftrag ausgeführt wurde.

Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

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

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs**.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

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

Wiederherstellung einer SQL Server-Datenbank aus dem sekundären Storage

Sie können die gesicherten SQL Server Datenbanken von den physischen LUNs (RDM, iSCSI oder FCP) auf einem sekundären Speichersystem wiederherstellen. Die Funktion „Restore“ ist ein mehrphasiger Prozess, bei dem alle Daten und Protokollseiten von einem bestimmten SQL Server Backup im sekundären Storage-System in eine angegebene Datenbank kopiert werden.

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 Assistenten Wiederherstellen werden im grundlegenden Wiederherstellungsprozess erläutert. In den folgenden Informationen werden einige der Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

Über diese Aufgabe

Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

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 Dropdown-Liste **Ansicht** die Option **Datenbank** oder **Ressourcengruppe** aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.

   Die Topologieseite für die Datenbank- oder Ressourcengruppe wird angezeigt.
4. Wählen Sie im Abschnitt Kopien verwalten aus dem sekundären Speichersystem (gespiegelt oder Tresor) **Backups** aus.
5. Wählen Sie das Backup aus der Liste aus, und klicken Sie dann auf  .
6. Wählen Sie auf der Seite Standort das Zielvolume für die Wiederherstellung der ausgewählten Ressource aus.
7. Schließen Sie den Wiederherstellungs-Assistenten ab, überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Wenn Sie eine Datenbank auf einem anderen Pfad wiederherstellen, der von anderen Datenbanken gemeinsam genutzt wird, sollten Sie eine vollständige Backup- und Backup-Verifizierung durchführen, um zu bestätigen, dass Ihre wiederhergestellte Datenbank frei von Beschädigungen auf physischer Ebene ist.

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   PS C:\> Open-Smconnection
   ```
2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

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

Datenbanken der Verfügbarkeitsgruppe erneut erstellen

Erneutes Seeding ist eine Option zur Wiederherstellung von Datenbanken der Availability Group (AG). Sollte die Synchronisierung einer sekundären Datenbank mit der primären Datenbank in einer AG nicht mehr synchronisiert werden, können Sie die sekundäre Datenbank erneut speichern.

Bevor Sie beginnen

- Sie müssen ein Backup der sekundären AG-Datenbank erstellt haben, die Sie wiederherstellen möchten.
- Der SnapCenter-Server und der Plug-in-Host müssen dieselbe SnapCenter-Version installiert haben.

Über diese Aufgabe

- Ein erneutes Seeding von primären Datenbanken kann nicht durchgeführt werden.
- Ein erneutes Seeding kann nicht ausgeführt werden, wenn die Datenbank des Replikats aus der Verfügbarkeitsgruppe entfernt wird. Wenn das Replikat entfernt wird, schlägt der erneute Seeding fehl.
- Während Sie den Vorgang für erneutes Seeding in der Datenbank der SQL Availability Group ausführen, sollten Sie keine Protokoll-Backups auf den Replikatdatenbanken dieser Availability Group-Datenbank auslösen. Wenn Sie während des erneuten Seeding-Vorgangs Protokollsicherungen auslösen, schlägt der Vorgang des erneuten Seeding mit der Spiegeldatenbank fehl. „Database_Name“ verfügt über unzureichende Transaktions-Log-Daten, um die Backup-Kette der Hauptdatenbank-Fehlermeldung zu erhalten.

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

Überwachung von Restore-Vorgängen bei SQL-Ressourcen

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

Über diese Aufgabe

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

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.

b. Geben Sie das Start- und Enddatum an.

c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.

d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.

e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.

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

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

Wiederherstellungsvorgänge für SQL-Ressourcen abbrechen

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.

Von der…	Aktion
Aktivitätsbereich	1. Nachdem Sie den Wiederherstellungsvorgang gestartet haben, klicken Sie auf das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

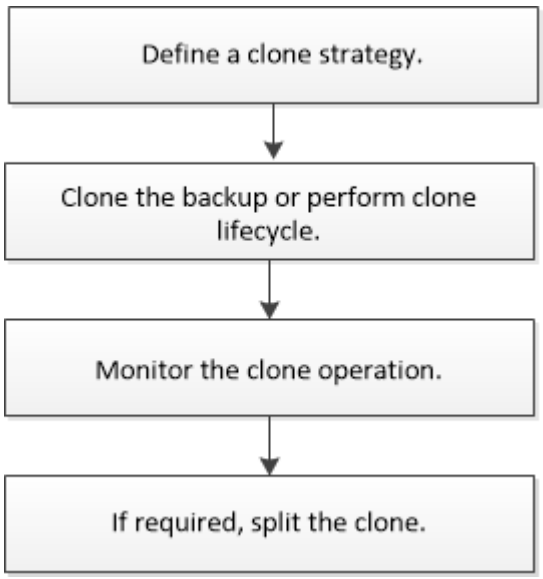
Klonen von SQL Server Datenbankressourcen

Klon-Workflow

Vor dem Klonen von Datenbankressourcen aus einem Backup müssen Sie mehrere Aufgaben mit SnapCenter Server ausführen. Beim Datenbankklonen wird eine zeitpunktgenaue Kopie einer Produktionsdatenbank oder des zugehörigen Backup-Satzes erstellt. Sie können Datenbanken klonen, um Funktionen zu testen, die mit der aktuellen Datenbankstruktur und dem Inhalt während der Anwendungsentwicklungszyklen implementiert werden müssen, um die Werkzeuge zur Datenextraktion und -Bearbeitung beim Befüllen von Data Warehouses zu verwenden oder Daten, die versehentlich gelöscht oder geändert wurden, wiederherzustellen.

Bei einem Datenbankklonen werden Berichte auf Basis der Job-IDs erstellt.

Im folgenden Workflow ist die Reihenfolge aufgeführt, in der Sie die Klonvorgänge ausführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch"

Weitere Informationen

"Klonen aus einem Backup der SQL Server Datenbank"

"Führen Sie Den Klon-Lebenszyklus Durch"

"Der Klonvorgang kann fehlschlagen oder längere Zeit zum Abschließen mit dem Standardwert für TCP_TIMEOUT benötigen"

Klonen aus einem Backup der SQL Server Datenbank

Sie können das Backup einer SQL Server Datenbank mit SnapCenter klonen. Wenn Sie auf eine ältere Version der Daten zugreifen oder diese wiederherstellen möchten, können Sie Datenbank-Backups nach Bedarf klonen.

Bevor Sie beginnen

- Sie sollten sich auf den Datenschutz vorbereiten, indem Sie Aufgaben wie das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Speichersystem abschließen.
- Sie sollten Datenbanken oder Ressourcengruppen gesichert haben.
- Der Sicherungstyp wie Mirror, Vault oder Mirror-Vault für Daten-LUN und Protokoll-LUN sollte dieselben sein, um sekundäre Lokatoren beim Klonen zu einem alternativen Host mithilfe von Protokoll-Backups zu erkennen.
- Wenn das gemountete Klonlaufwerk während eines SnapCenter Klonvorgangs nicht gefunden werden kann, sollten Sie den Parameter CloneRetryTimeout von SnapCenter Server in 300 ändern.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.

Über diese Aufgabe

- Stellen Sie beim Klonen auf eine eigenständige Datenbankinstanz sicher, dass der Mount-Point-Pfad vorhanden ist und dass es sich um eine dedizierte Festplatte handelt.
- Beim Klonen in eine Failover Cluster-Instanz (FCI) stellen Sie sicher, dass die Mount-Punkte vorhanden sind, dass es sich um eine freigegebene Festplatte handelt, und der Pfad und die FCI sollten zur gleichen SQL-Ressourcengruppe gehören.
- Stellen Sie sicher, dass nur ein VFC- oder FC-Initiator mit jedem Host verbunden ist. Der Grund dafür ist, dass SnapCenter nur einen Initiator pro Host unterstützt.
- Wenn sich die Quelldatenbank oder die Zielinstanz auf einem gemeinsam genutzten Cluster-Volume (csv) befindet, befindet sich die geklonte Datenbank auf dem csv.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

Stellen Sie für virtuelle Umgebungen (VMDK/RDM) sicher, dass der Bereitstellungspunkt eine dedizierte Festplatte ist.

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

UI von SnapCenter

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann **SnapCenter Plug-in für SQL Server** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.

   Das Klonen eines Backups einer Instanz wird nicht unterstützt.

3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** das Backup entweder aus dem primären oder sekundären (gespiegelten oder gewölbten) Speichersystem aus.
5. Wählen Sie die Sicherung aus, und wählen Sie dann * *  .
6. Führen Sie auf der Seite **Clone Options** die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Kloninstanz	Wählen Sie eine Kloninstanz aus, zu der Sie das Datenbank-Backup klonen möchten. Diese SQL-Instanz muss sich auf dem angegebenen Klon-Server befinden.
Suffix klonen	Geben Sie ein Suffix ein, das an den Namen der Klondatei angehängt wird, um zu identifizieren, dass die Datenbank ein Klon ist. Beispiel: *db1_Clone*. Wenn Sie an demselben Speicherort wie die Originaldatenbank klonen, müssen Sie ein Suffix bereitstellen, um die geklonte Datenbank von der ursprünglichen Datenbank zu unterscheiden. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Automatisches Zuweisen von Mount-Punkten oder automatische Zuweisung von Volume-Mount-Punkten unter Pfad	Legen Sie fest, ob unter einem Pfad automatisch ein Mount-Punkt oder ein Volume-Mount-Punkt zugewiesen werden soll. Automatisches Zuweisen von Volume-Mount-Punkt unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht es Ihnen, ein bestimmtes Verzeichnis bereitzustellen. Die Mount-Punkte werden innerhalb dieses Verzeichnisses erstellt. Bevor Sie diese Option auswählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich eine Datenbank im Verzeichnis befindet, befindet sich die Datenbank nach dem Mount-Vorgang in einem ungültigen Status.

7. Wählen Sie auf der Seite Protokolle eine der folgenden Optionen aus:

Für dieses Feld…	Tun Sie das…
Keine	Wählen Sie diese Option, wenn Sie nur das vollständige Backup ohne Logs klonen möchten.
Alle Log-Backups	Wählen Sie diese Option, um alle verfügbaren Protokoll-Backups zu klonen, die nach der vollständigen Sicherung datiert sind.
Durch Backups bis protokollieren	Wählen Sie diese Option, um die Datenbank auf Basis der Backup-Protokolle zu klonen, die bis zum Backup-Protokoll mit dem ausgewählten Datum erstellt wurden.
Nach einem bestimmten Datum bis	Geben Sie Datum und Uhrzeit an, nach denen die Transaktionsprotokolle nicht auf die geklonte Datenbank angewendet werden. Dieser Point-in-Time-Klon stoppt den Klon der Transaktions-Log-Einträge, die nach dem angegebenen Datum und der angegebenen Zeit aufgezeichnet wurden.

8. Geben Sie auf der Seite **Script** das Skript-Timeout, den Pfad und die Argumente des Prescript oder Postscript ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.

   Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares 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-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

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

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

   Für EMS finden Sie weitere Informationen unter "EMS-Datenerfassung managen"

10. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Nachdem Sie fertig sind

Nach dem Erstellen des Klons sollten Sie ihn nicht mehr umbenennen.

Verwandte Informationen

"Der Klonvorgang kann fehlschlagen oder längere Zeit zum Abschließen mit dem Standardwert für TCP_TIMEOUT benötigen"

"Der Datenbankklon für die Failover-Cluster-Instanz ist fehlgeschlagen"

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Backups auf, die mit dem Cmdlet "Get-SmBackup" oder "Get-SmResourceGroup" geklont werden können.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

In diesem Beispiel werden Informationen über eine bestimmte Ressourcengruppe, ihre Ressourcen und zugehörige 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}
HostResourceMaping : {}
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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup mit dem Cmdlet "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 für eine angegebene 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 Clone-Jobs mit dem Cmdlet Get-SmCloneReport an.

   In diesem Beispiel wird ein Klonbericht für die angegebene Job-ID angezeigt:

```
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}
```

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

Führen Sie Den Klon-Lebenszyklus Durch

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 ein Backup regelmäßig klonen, können Sie mit dem Klon Applikationen entwickeln, Daten ausfüllen oder Daten wiederherstellen.

SnapCenter ermöglicht die Planung mehrerer Klonvorgänge zur gleichzeitigen Ausführung über mehrere Server hinweg.

Bevor Sie beginnen

- Stellen Sie beim Klonen auf eine eigenständige Datenbankinstanz sicher, dass der Mount-Point-Pfad vorhanden ist und dass es sich um eine dedizierte Festplatte handelt.
- Beim Klonen in eine Failover Cluster-Instanz (FCI) stellen Sie sicher, dass die Mount-Punkte vorhanden sind, dass es sich um eine freigegebene Festplatte handelt, und der Pfad und die FCI sollten zur gleichen SQL-Ressourcengruppe gehören.
- Wenn sich die Quelldatenbank oder die Zielinstanz auf einem gemeinsam genutzten Cluster-Volume (csv) befindet, befindet sich die geklonte Datenbank auf dem csv.

Stellen Sie für virtuelle Umgebungen (VMDK/RDM) sicher, dass der Bereitstellungspunkt eine dedizierte Festplatte ist.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

- Die meisten Felder auf den Seiten des Clone Lifecycle Wizard sind selbsterklärend. In den folgenden Informationen werden die Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.
- Wenn Sie für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die aus den manipulationssicheren Snapshots erstellten Klone die Ablaufdatum von SnapLock. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer 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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** 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 durch:

Für dieses Feld…	Tun Sie das…
Auftragsname klonen	Geben Sie den Namen des Jobs für den Lebenszyklus des Klons an, der die Überwachung und Änderung des Lebenszyklusjobs unterstützt.
Klonserver	Wählen Sie den Host aus, auf dem der Klon platziert werden soll.
Kloninstanz	Wählen Sie die Kloninstanz aus, zu der Sie die Datenbank klonen möchten. Diese SQL-Instanz muss sich auf dem angegebenen Klon-Server befinden.

Für dieses Feld…	Tun Sie das…
Suffix klonen	Geben Sie ein Suffix ein, das an die Klondatenbank angehängt wird, um das es sich um einen Klon handelt. Jede SQL-Instanz, die zum Erstellen einer Clone-Ressourcengruppe verwendet wird, muss über einen eindeutigen Datenbanknamen verfügen. Wenn die Clone Resource Group beispielsweise eine Quelldatenbank „db1“ aus einer SQL-Instanz „inst1“ enthält und „db1“ in „inst1“ geklont wurde, sollte der Name der Klondatenbank „ db1*Clone*“ lauten. „Clone“ ist ein vom Benutzer definiertes Suffix, da die Datenbank in derselben Instanz geklont wird. Wenn “db1” zur SQL-Instanz „inst2“ geklont wird, kann der Name der Klondatenbank „db1“ bleiben (das Suffix ist optional), da die Datenbank auf eine andere Instanz geklont wird.
Automatisches Zuweisen von Mount-Punkten oder automatische Zuweisung von Volume-Mount-Punkten unter Pfad	Legen Sie fest, ob unter einem Pfad automatisch ein Mount-Punkt oder ein Volume-Mount-Punkt zugewiesen werden soll. Wenn Sie die Option auswählen, einen Volume-Bereitstellungspunkt unter einem Pfad automatisch zuzuweisen, können Sie ein bestimmtes Verzeichnis angeben. Die Mount-Punkte werden innerhalb dieses Verzeichnisses erstellt. Bevor Sie diese Option auswählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich eine Datenbank im Verzeichnis befindet, befindet sich die Datenbank nach dem Mount-Vorgang in einem ungültigen Status.

5. Wählen Sie auf der Seite Speicherort einen Speicherort aus, um einen Klon zu erstellen.
6. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.

   Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

   Das Standard-Skript-Timeout beträgt 60 Sekunden.

7. Führen Sie auf der Seite Zeitplan eine der folgenden Aktionen durch:
   - Wählen Sie **Jetzt ausführen** aus, wenn Sie den Klon-Job sofort ausführen möchten.
   - Wählen Sie **Configure Schedule** aus, wenn Sie bestimmen möchten, wie häufig der Klonvorgang stattfinden soll, wann der Klonzeitplan beginnen soll, an welchem Tag der Klonvorgang stattfinden soll, wann der Zeitplan abläuft und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.

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

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

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

   Für EMS finden Sie weitere Informationen unter "EMS-Datenerfassung managen"

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

Sie sollten den Klonprozess über die Seite **Monitor** > **Jobs** überwachen.

Überwachen Sie die Klonvorgänge von SQL Datenbanken

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

Über diese Aufgabe

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

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

Schritte

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

Klonvorgänge für SQL-Ressourcen abbrechen

Sie können Klonvorgänge in die Warteschlange abbrechen.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Klonvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Klonvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen ausgeführten Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Klonvorgänge abzubrechen.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Vorgang aus, und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Klonvorgangs auf  das Teilfenster „Aktivität“, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite **Job Details** auf **Job abbrechen**.

Teilen Sie einen Klon auf

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

Über diese Aufgabe

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

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

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht

mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

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

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

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

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

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

   Beispiel:

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

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

Verwandte Informationen

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

Schutz von SAP HANA Datenbanken

SnapCenter Plug-in für SAP HANA Datenbanken

SnapCenter-Plug-in für SAP HANA-Datenbank – Überblick

Das SnapCenter Plug-in für SAP HANA Database ist eine Host-seitige Komponente der NetApp SnapCenter Software, die ein applikationsgerechtes Datensicherungsmanagement für SAP HANA Datenbanken ermöglicht. Das Plug-in für SAP HANA Database automatisiert das Backup, Restore und Klonen von SAP HANA Datenbanken in der SnapCenter Umgebung.

SnapCenter unterstützt einzelne Container und mandantenfähige Datenbank-Container (MDC). Sie können das Plug-in für SAP HANA Datenbanken 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 zentrale Host-Plug-in kann mehrere HANA-Datenbanken über verschiedene Hosts hinweg managen.

Wenn das Plug-in für SAP HANA Datenbank installiert ist, kann SnapCenter mit NetApp SnapMirror Technologie verwendet werden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Mithilfe des Plug-ins in mit NetApp SnapVault Technologie lässt sich darüber hinaus eine Disk-to-Disk-Backup-Replizierung zur Einhaltung von Standards durchführen.

Das Plug-in für SAP HANA Datenbank unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]). So können Business-Services auch bei einem vollständigen Standortausfall weiterlaufen und Applikationen unterstützen, bei denen ein transparentes Failover mithilfe einer sekundären Kopie möglich ist. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.

Was Sie mit dem SnapCenter Plug-in für SAP HANA Database tun können

Wenn Sie das Plug-in für SAP HANA Datenbank in Ihrer Umgebung installieren, können Sie mit SnapCenter SAP HANA Datenbanken und deren Ressourcen sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Hinzufügen von Datenbanken:
- Backups erstellen.
- Restore aus Backups:
- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

SnapCenter Plug-in für SAP HANA Database Funktionen

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Zur Nutzung mit dem Plug-in für SAP HANA-Datenbank

verwenden Sie die grafische Benutzeroberfläche von SnapCenter.

- **Einheitliche grafische Benutzeroberfläche**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore- und Klonvorgänge über alle Plug-ins hinweg, die zentralisierte Berichterstellung, die Schnellübersicht über Dashboard-Ansichten, die Einrichtung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Jobs in allen Plug-ins.

- **Automatisierte zentrale Verwaltung**

  Sie können Backup-Vorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Unterbrechungsfreie NetApp Snapshot Kopie-Technologie**

  SnapCenter verwendet NetApp Snapshot Technologie mit dem Plug-in für SAP HANA Database, um Ressourcen zu sichern.

Die Nutzung des Plug-ins für SAP HANA Database bietet darüber hinaus folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktgenauer Kopien von Ressourcen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Unterstützung der Snapshot-Funktion von ONTAP für Konsistenzgruppen (CG) beim Erstellen von Backups.
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Möglichkeit zum Erstellen von Snapshots mit externen Befehlen.
- Unterstützung für dateibasierte Backups.
- Unterstützung für Linux LVM auf XFS-Dateisystem.

Storage-Typen, die vom SnapCenter Plug-in für SAP HANA Database unterstützt werden

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines (VMs). Sie müssen die Unterstützung Ihres Speichertyps überprüfen, bevor Sie das SnapCenter-Plug-in für SAP HANA Database installieren.

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datastores • VMDKs auf VMFS erstellt • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Minimale ONTAP-Berechtigungen für SAP HANA-Plug-in erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun erstellen
  - lun erstellen
  - lun erstellen
  - lun löschen

- lun Initiatorgruppe hinzufügen
- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen

    - Show-Disk-Nutzung für Volume-Dateien
    - Volume ist offline
    - Das Volume ist online
    - Volume-Änderung
    - Erstellen von Volume-qtree
    - Volume qtree löschen
    - Änderung des Volume-qtree
    - Volume-qtree anzeigen
    - Volume-Einschränkung
    - Volumen anzeigen
    - Erstellen von Volume-Snapshots
    - Volume Snapshot löschen
    - Ändern des Volume-Snapshots
    - Volume Snapshot modify-snaplock-expiry-time
    - Umbenennung von Volume-Snapshots
    - Wiederherstellung von Volume Snapshots
    - Restore-Datei für Volume Snapshots
    - Volume-Snapshot werden angezeigt
    - Volume-Aufhängung nicht verfügbar
    - cifs von vserver
    - erstellung von cifs-Freigaben von vserver
    - cifs-Freigabe von vserver: Löschen
    - vserver cifs shadowcopy anzeigen
    - cifs-Freigabe von vserver wird angezeigt
    - vserver cifs zeigen
    - vserver Exportrichtlinie
    - Erstellung von vserver Exportrichtlinien
    - vserver: Löschen der Exportrichtlinie
    - Erstellung von vserver Export-Policy-Regel
    - vserver: Export-Policy-Regel anzeigen
    - vserver Export-Policy wird angezeigt
    - vserver iscsi
    - vserver iscsi-Verbindung wird angezeigt
    - vserver zeigen
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle
    - Netzwerkschnittstelle wird angezeigt

- vserver

Vorbereiten der Storage-Systeme für SnapMirror und SnapVault Replizierung für SAP HANA Datenbanken

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie für SAP HANA Datenbanken

Backup-Strategie für SAP HANA Datenbanken definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre Ressourcen erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Über diese Aufgabe

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.
2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Entscheiden Sie, ob Sie eine Richtlinie für auf Snapshot Kopien basierende erstellen möchten, um applikationskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie die Integrität der Datenbank überprüfen möchten.
6. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
7. Bestimmen Sie den Aufbewahrungszeitraum für die Snapshots auf dem Quell-Storage-System und dem SnapMirror Ziel.
8. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Automatische Ermittlung von Ressourcen auf Linux-Host

Ressourcen sind SAP HANA Datenbanken und nicht-Daten-Volumes auf dem Linux-Host, die von SnapCenter gemanagt werden. Nach der Installation des SnapCenter-Plug-ins für SAP HANA-Datenbank 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:

- Einzelne Container

  Nach der Installation oder dem Upgrade des Plug-ins werden die einzelnen Container-Ressourcen in einem zentralen Host-Plug-in als manuell zusätzliche Ressourcen fortgesetzt.

  Nach der Installation oder dem Upgrade des Plug-ins werden die SAP HANA Datenbanken automatisch nur auf den SAP HANA Linux-Hosts erkannt, die direkt bei SnapCenter registriert sind.

- Mandantenfähiger Datenbank-Container (MDC)

  Nach der Installation oder dem Upgrade des Plug-ins werden die MDC-Ressourcen auf einem zentralen Host-Plug-in als manuell hinzugefügte Ressource fortgesetzt.

  Nach dem Upgrade auf SnapCenter 4.3 müssen Sie weiterhin die MDC-Ressourcen auf dem zentralen Host-Plug-in manuell hinzufügen.

  Bei direkt in SnapCenter registrierten SAP HANA Linux-Hosts wird durch die Installation oder ein Upgrade des Plug-ins eine automatische Ermittlung der Ressourcen auf dem Host ausgelöst. 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 ermittelt und in SnapCenter registriert. Die neue Ressource befindet sich im Status gesperrt.

  Wenn sich beispielsweise in SnapCenter 4.2 die 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 ermittelt werden, werden die Datensicherungsvorgänge von diesen Ressourcen nicht unterstützt.

- HANA Konfiguration für mehrere Hosts
- Mehrere Instanzen auf demselben Host
- Mehrschichtige Scale-out HANA System Replication
- Kaskadierte Replikationsumgebung im System Replication-Modus

Art der unterstützten Backups

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt dateibasierte Backups und auf Snapshot Kopien basierende Backup-Typen für SAP HANA Datenbanken.

Dateibasiertes Backup

Dateibasierte Backups bestätigen die Integrität der Datenbank. Sie können den dateibasierten Backup-Vorgang in bestimmten Intervallen planen. Es werden nur aktive Mandanten gesichert. Sie können dateibasierte Backups nicht aus SnapCenter wiederherstellen und klonen.

Backup auf Basis von Snapshot Kopien

Auf Snapshot Kopien basierende Backups nutzen die NetApp Snapshot Technologie, um Online-schreibgeschützte Kopien der Volumes zu erstellen, auf denen sich die SAP HANA Datenbanken befinden.

So verwendet das SnapCenter Plug-in für SAP HANA Database Snapshots von Konsistenzgruppen

Sie können das Plug-in verwenden, um Snapshots von Konsistenzgruppen für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes beherbergen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe ist simultane Snapshots mehrerer Volumes und bietet konsistente Kopien einer Gruppe von Volumes.

Sie können auch die Wartezeit für die konsistente Gruppierung von Snapshots durch den Storage Controller angeben. Die verfügbaren Optionen für Wartezeiten sind **dringend**, **Medium** und **entspannt**. Sie können auch die WAFL-Synchronisierung (Write Anywhere File Layout) während des Snapshot-Vorgangs einer konsistenten Gruppe aktivieren oder deaktivieren. WAFL Sync verbessert die Performance eines Snapshots von Konsistenzgruppen.

SnapCenter managt die allgemeine Ordnung und Sauberkeit von Protokoll- und Daten-Backups

SnapCenter managt die allgemeine Ordnung und Sauberkeit der Protokoll- und Daten-Backups auf den Ebenen des Storage-Systems und des Filesystems und innerhalb des SAP HANA Backup-Katalogs.

Die Snapshots auf dem primären oder sekundären Speicher und die entsprechenden Einträge im SAP HANA-Katalog werden auf Basis der Aufbewahrungseinstellungen gelöscht. Die SAP HANA-Katalogeinträge werden auch beim Backup und beim Löschen von Ressourcengruppen gelöscht.

Überlegungen bei der Ermittlung von Backup-Zeitplänen für die SAP HANA Datenbank

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, die Service Level Agreement (SLA) und den Recovery Point Objective (RPO).

Backup-Zeitpläne haben zwei Teile:

- Backup-Häufigkeit (Häufigkeit der Durchführung von Backups)

  Die Backup-Häufigkeit, die auch als Zeitplantyp für einige Plug-ins bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau dann, wenn Backups durchgeführt werden sollen

  Backup-Zeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird

Anzahl der für SAP HANA-Datenbanken erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Backup-Namenskonventionen für SAP HANA Datenbanken

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Restore- und Recovery-Strategie für SAP HANA Datenbanken

Restore- und Recovery-Strategie für SAP HANA-Ressourcen definieren

Sie müssen eine Strategie definieren, bevor Sie Ihre Datenbank wiederherstellen und wiederherstellen, damit Restore- und Recovery-Vorgänge erfolgreich durchgeführt werden können.

Schritte

1. Legen Sie die Wiederherstellungsstrategien fest, die für manuell hinzugefügte SAP HANA-Ressourcen unterstützt werden
2. Legen Sie die Wiederherstellungsstrategien fest, die für automatisch erkannte SAP HANA-Datenbanken unterstützt werden
3. Geben Sie die Art der Recovery-Vorgänge an, die Sie ausführen möchten.

Arten von Wiederherstellungsstrategien werden für manuell hinzugefügte SAP HANA-Ressourcen unterstützt

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte SAP HANA-Ressourcen. Manuell hinzugefügte SAP HANA-Ressourcen können nicht wiederhergestellt werden.

Manuell hinzugefügte SAP HANA-Ressourcen können nicht wiederhergestellt werden.

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her

Wenn die Ressource Volumes oder qtrees enthält, werden die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

Wiederherstellung auf Dateiebene

- Wiederherstellung von Dateien aus Volumes, qtrees oder Verzeichnissen
- Stellt nur die ausgewählten LUNs wieder her

Arten von Wiederherstellungsstrategien werden für automatisch erkannte SAP HANA-Datenbanken unterstützt

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für automatisch erkannte SAP HANA Datenbanken.

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her
  - Die Option **Volume revert** sollte ausgewählt werden, um das gesamte Volume wiederherzustellen.

> Wenn die Ressource Volumes oder qtrees enthält, werden die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

Mandanten-Datenbank

- Stellt die Mandantendatenbank wieder her

Wenn die Option **Tenant Database** ausgewählt ist, müssen HANA Studio oder HANA Recovery Scripts außerhalb von SnapCenter verwendet werden, um den Recovery-Vorgang durchzuführen.

Arten von Wiederherstellungsvorgängen für automatisch erkannte SAP HANA-Datenbanken

SnapCenter unterstützt Volume-basierte SnapRestore (VBSR), Single File SnapRestore und Connect-and-Copy Restore-Typen für automatisch erkannte SAP HANA Datenbanken.

Volume-basiertes SnapRestore (VBSR) wird in NFS-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn das für die Wiederherstellung ausgewählte Backup auf Versionen vor SnapCenter 4.3 durchgeführt wird, und nur, wenn die Option **Complete Resource**ausgewählt ist
- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und wenn die Option **Volume revert** ausgewählt ist

Ein Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn die für die Wiederherstellung ausgewählte Sicherung in SnapCenter 4.3 erstellt wird und nur die Option **vollständige Ressource** ausgewählt ist
- Für mandantenfähige Datenbank-Container (MDC), wenn das für die Wiederherstellung ausgewählte Backup auf SnapCenter 4.3 übernommen wird, und die Option **Tenant Database** ausgewählt ist
- Wenn der ausgewählte Backup von einem sekundären Standort SnapMirror oder SnapVault stammt und die Option **Complete Resource** ausgewählt ist

Ein Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn Backups auf Versionen vor SnapCenter 4.3 erstellt werden und nur dann, wenn die Option **Complete Resource** ausgewählt ist
- Wenn Backups in SnapCenter 4.3 erstellt werden und nur dann, wenn die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem sekundären Standort SnapMirror oder SnapVault ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Connect-and-Copy-Based Restore 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

> **Complete Resource**, **Volume Revert** und **Tenant Database** Optionen sind auf der Seite „Bereich wiederherstellen“ verfügbar.

Arten von Recovery-Vorgängen unterstützt für SAP HANA-Datenbanken

SnapCenter ermöglicht Ihnen die Durchführung verschiedener Recovery-Vorgänge für SAP HANA Datenbanken.

- Wiederherstellung der Datenbank im aktuellsten Zustand
- Wiederherstellung der Datenbank zu einem bestimmten Zeitpunkt

  Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.

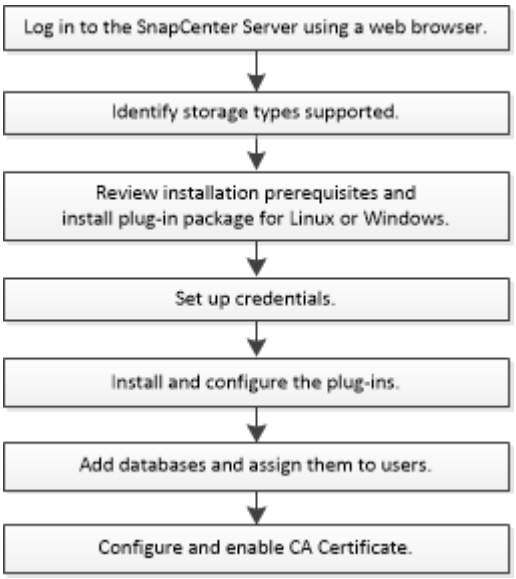
- Wiederherstellung der Datenbank in einem bestimmten Daten-Backup

SnapCenter bietet auch die Option „kein Recovery“ für SAP HANA Datenbanken.

Bereiten Sie sich auf die Installation des SnapCenter-Plug-ins für die SAP HANA-Datenbank vor

Installationsworkflow des SnapCenter Plug-ins für SAP HANA Database

Sie sollten das SnapCenter Plug-in für SAP HANA Database installieren und einrichten, wenn Sie SAP HANA Datenbanken schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter Plug-ins für SAP HANA Database

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Das SnapCenter Plug-in für SAP HANA Database ist sowohl in Windows als auch in Linux Umgebungen verfügbar.

- Sie müssen Java 11 auf Ihrem Host installiert haben.

  IBM Java wird nicht unterstützt.

- Sie müssen das interaktive Terminal (HDBSQL-Client) der SAP HANA-Datenbank auf dem Host installiert haben.
- Für Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „`LocalSystem`“ ausgeführt werden. Dies ist das Standardverhalten, wenn Plug-in für SAP HANA Database als Domänenadministrator installiert wird.
- Unter Windows sollten Benutzer-Speicherschlüssel als SYSTEMBENUTZER erstellt werden.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört. Das SnapCenter Plug-in für Microsoft Windows wird standardmäßig mit dem SAP HANA Plug-in auf Windows Hosts implementiert.
- Für Linux-Host werden HDB Secure User Store-Schlüssel als HDBSQL OS-Benutzer aufgerufen.
- Der SnapCenter-Server sollte Zugriff auf den 8145-Port oder den benutzerdefinierten Port des Plug-ins für SAP HANA-Datenbank-Host haben.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Bei der Installation von Plug-in für 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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-Tool"

- Für SAP HANA-Datenbanken, die auf einem Linux-Host ausgeführt werden und das Plug-in für SAP HANA Database installieren, wird das SnapCenter-Plug-in für UNIX automatisch installiert.

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

Zusätzliche Befehle

Um einen zusätzlichen Befehl auf dem SnapCenter-Plug-in für SAP HANA auszuführen, müssen Sie ihn in die Datei *allowed_commands.config* einfügen.

- 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 eine separate Zeile ein, und bei den Befehlen wird die Groß-/Kleinschreibung nicht beachtet. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen („) einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: Montieren

Befehl: Umount

Befehl: „C:\Program Files\NetApp\SnapCreator commands\sdcli.exe“

Befehl: myscript.bat

Wenn die Datei *allowed_commands.config* nicht vorhanden ist, werden die Befehle oder die Ausführung des Skripts blockiert, und der Workflow schlägt mit dem folgenden Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Wenn der Befehl oder das Skript nicht in *allowed_commands.config* vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit folgendem Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Sie sollten keinen Platzhaltereintrag (*) verwenden, um alle Befehle zuzulassen.

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter 2.0 und höheren Versionen kann ein nicht-Root-Benutzer das SnapCenter Plug-ins-Paket für Linux installieren und das Plug-in-Verfahren 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Stellen Sie für den Benutzer, der nicht root ist, sicher, dass der Name des Benutzers, der nicht root ist, und

die Gruppe des Benutzers identisch sein sollten.

- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist. .

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Host-Anforderungen 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 Speicherplatz- und Größenanforderungen des Host-Systems vertraut sein.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit der Datensicherungsvorgänge. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Anmeldedaten für das SnapCenter-Plug-in für SAP HANA-Datenbank einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken oder Windows-Dateisystemen erstellen.

Über diese Aufgabe

- Linux-Hosts

Sie müssen Anmeldedaten für die Installation von Plug-ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen zu erstellen, bevor Sie Hosts bereitstellen und Plug-ins installieren.

- Windows Hosts

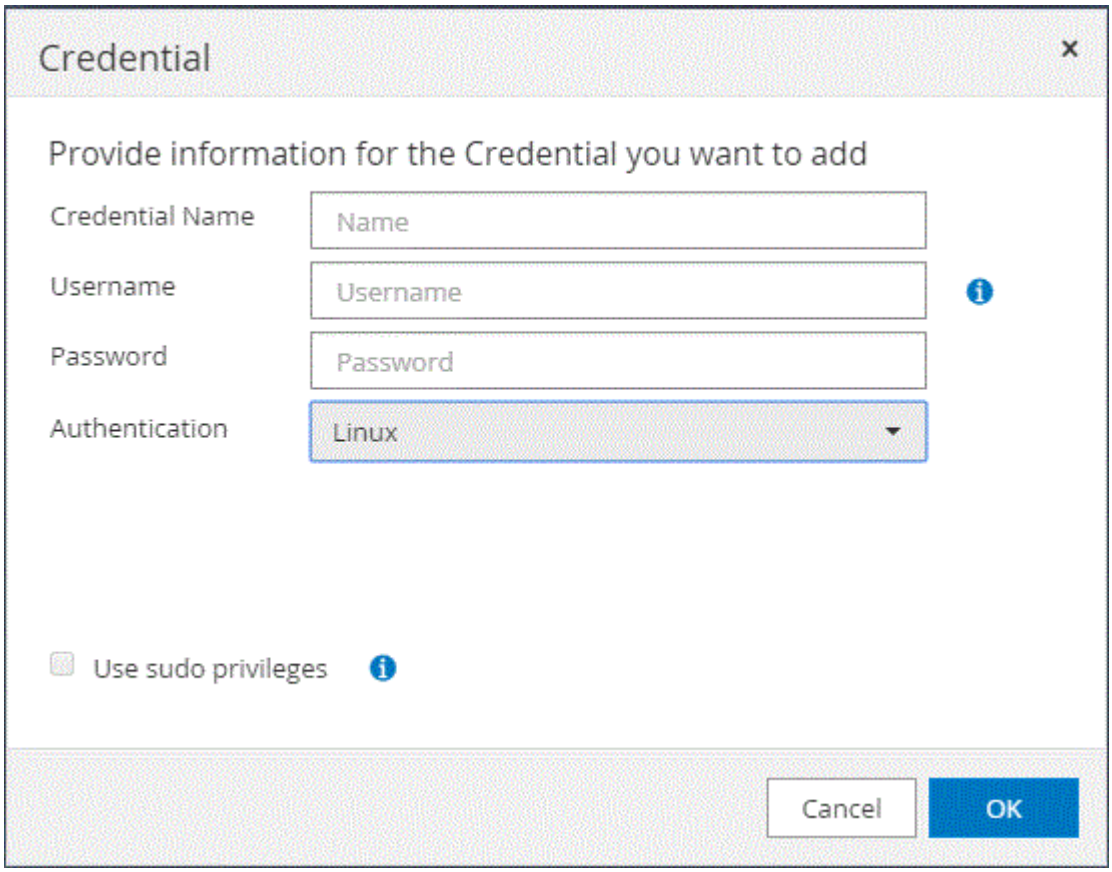
  Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.

  Sie müssen die Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.



4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.
Benutzername	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username* Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.

Für dieses Feld…	Tun Sie das…
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten. Nur für Linux-Benutzer verfügbar.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

      Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

   b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Das SnapCenter-Plug-in für SAP HANA Datenbanken installieren

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen Hosts über die Seite SnapCenter Add Host hinzufügen hinzufügen und dann die Plug-ins-Pakete installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und Plug-in-Pakete für einen einzelnen Host oder für ein 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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zum Verwalten von Hosts.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfiguration des Gruppenverwaltungsservice-Kontos unter Windows Server 2016 oder höher für SAP HANA"

Über diese Aufgabe

- Sie können einen SnapCenter-Server nicht als Plug-in-Host zu einem anderen SnapCenter-Server hinzufügen.
- Für SAP HANA System Replication zur Ermittlung von Ressourcen auf primären und sekundären Systemen wird empfohlen, sowohl das primäre als auch das sekundäre System mit Root- oder Sudo-Benutzer hinzuzufügen.

Schritte

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

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ aus: • Windows • Linux Das Plug-in für SAP HANA ist auf dem HDBSQL-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System installiert sein.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den Hostnamen der Kommunikation ein. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie müssen den HDBSQL-Client und den HDBUserStore auf diesem Host konfigurieren.
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Installationspfad	Das Plug-in für SAP HANA ist auf dem HDBSQL-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System installiert sein. • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. Optional können Sie den Pfad anpassen. • Für das SnapCenter Plug-ins-Paket für Linux lautet der Standardpfad: /Opt/NetApp/snapcenter. Optional können Sie den Pfad anpassen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden mit den Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\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-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

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

9. Überwachen Sie den Installationsfortschritt.

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

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 gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

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

   Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Installieren Sie das SnapCenter-Plug-in für SAP HANA-Datenbanken auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten das SnapCenter-Plug-in für SAP HANA-Datenbank über die SnapCenter-Benutzeroberfläche installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie das Plug-in für SAP HANA-Datenbank entweder im Konsolenmodus oder im Silent-Modus installieren, indem Sie die Befehlszeilenschnittstelle (CLI) verwenden.

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 SAP HANA Database installieren, muss die Anforderungen der abhängigen Software, der Datenbank und des Betriebssystems erfüllen.

  Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu unterstützten Konfigurationen.

  https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT

- Das SnapCenter-Plug-in für SAP HANA-Datenbank ist Teil des SnapCenter Plug-ins-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins Paket für Linux installieren, sollten Sie bereits SnapCenter auf einem Windows-Host installiert haben.

Schritte

1. Kopieren Sie das SnapCenter Plug-ins-Paket für die Linux-Installationsdatei (snapcenter_linux_Host_Plugin.bin) aus C:\ProgramData\NetApp\SnapCenter\Paket-Repository auf den Host, auf dem Sie das Plug-in für SAP HANA-Datenbank installieren möchten.

   Sie können von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 HTTPS-Kommunikationsport SMCore 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 das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
   - 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.

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

Überwachen Sie den Status der Installation des Plug-ins für SAP HANA

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

Über diese Aufgabe

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

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

Schritte

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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 für den SnapCenter-SAP HANA-Plug-ins-Service 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.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

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

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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen 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. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.

7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das Standardkennwort für den 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 Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
   Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
   einfachen Namen:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
   agent.properties.
   ```

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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 SnapCenter-Plug-Ins

Über diese Aufgabe

- 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 mit dem Schlüssel CRL_PATH ändern und aktualisieren.

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

Konfigurieren des CA-Zertifikats für den SnapCenter-SAP HANA-Plug-ins-Service 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 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 ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

   Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

   C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

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

   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: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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 enthält: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

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

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

Über diese Aufgabe

- Die neueste CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten 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* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

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

Konfigurieren Sie die CRL-Datei

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

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

Bereiten Sie sich auf die Datensicherung vor

Voraussetzungen für die Verwendung des SnapCenter-Plug-ins für SAP HANA-Datenbanken

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.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

  Sie müssen den Java-Pfad in der Umgebungspfadvariable des Host-Rechners festlegen.

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.
- Installieren Sie den HDBSQL-Client auf dem Host, auf dem Sie das Plug-in für SAP HANA-Datenbank installieren.

  Konfigurieren Sie die Benutzerspeicherschlüssel für die SAP HANA-Knoten, die Sie über diesen Host verwalten möchten.

- Wenn Sie ein SAP HANA-Datenbankbenutzerkonto verwenden, stellen Sie für die SAP HANA-Datenbank 2.0SPS05 sicher, dass Sie über die folgenden Berechtigungen zum Durchführen von Backup-, Wiederherstellungs- und Klonvorgängen im SnapCenter-Server verfügen:
  - Backup-Admin
  - Katalog gelesen
  - Datenbank-Backup-Administrator
  - Operator für Datenbank-Wiederherstellung

Verwendung von Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von SAP HANA Datenbanken

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind typischerweise 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 von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, Replizierung, Skripte und andere Eigenschaften von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

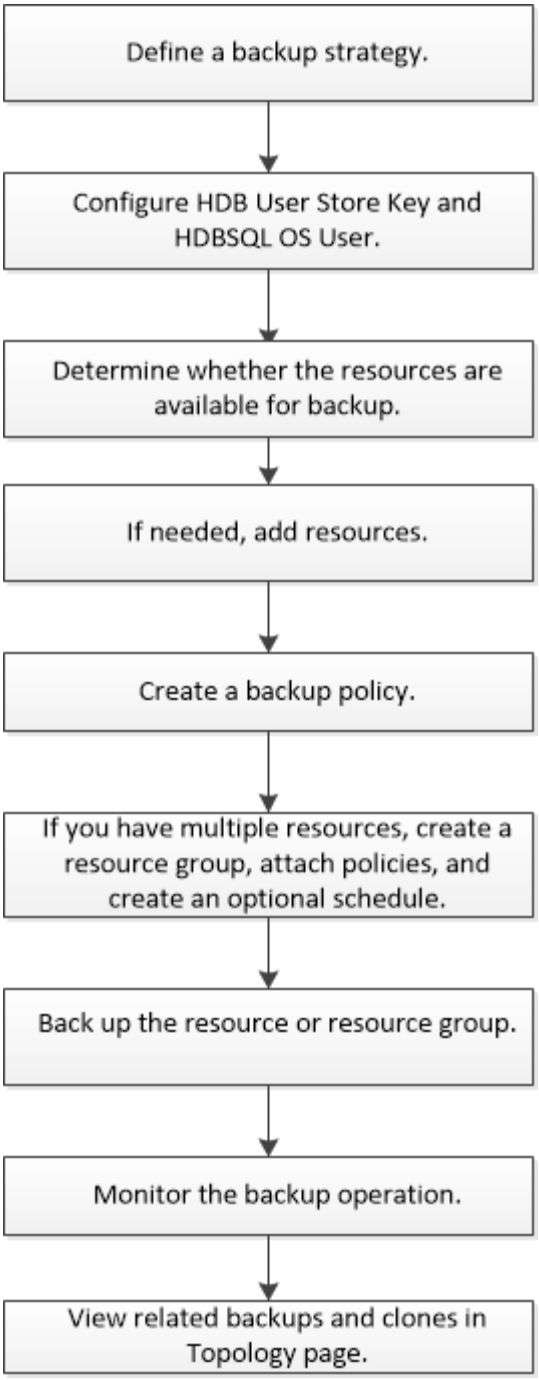
Stellen Sie sich eine Ressourcengruppe vor, die definiert, was Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Richtlinie, die definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts umfasst. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein vollständiges Backup durchführen.

SAP HANA-Ressourcen sichern

SAP HANA-Ressourcen sichern

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Datenbanken, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets. "SnapCenter Software Cmdlet Referenzhandbuch".

Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank

Sie müssen den HDB-Benutzerspeicherschlüssel und den HDBSQL OS-Benutzer konfigurieren, um Datenschutzvorgänge in SAP HANA-Datenbanken durchzuführen.

Bevor Sie beginnen

- Wenn in der SAP HANA-Datenbank nicht der HDB Secure User Store Key und der HDB SQL OS User konfiguriert sind, wird nur für die automatisch erkannten Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS Benutzer so konfigurieren, dass sie die Datenbank schützen oder einer Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.
- Sie müssen HDB SQL OS User konfigurieren, um auf die Systemdatenbank zugreifen zu können. Wenn HDB SQL OS User für den Zugriff auf nur die Mandantendatenbank konfiguriert ist, 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 **Ansicht** aus.
3. (Optional) Klicken Sie auf , und wählen Sie den Hostnamen aus.

   Sie können dann klicken , 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-Schlüssel für sicheren Benutzerspeicher ein.

   Der Plug-in-Hostname wird angezeigt und HDB SQL OS User wird automatisch in <sid>ADM eingetragen.
6. Klicken Sie auf **OK**.

Sie können die Datenbankkonfiguration auf der Seite Topology ändern.

Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor

Automatische Erkennung von Datenbanken

Ressourcen sind SAP HANA Datenbanken und nicht-Daten-Volumes auf dem Linux-Host, die von SnapCenter gemanagt werden. Diese Ressourcen können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge durchzuführen, nachdem die verfügbaren SAP HANA Datenbanken ermittelt wurden.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. die Installation des SnapCenter-Servers, das Hinzufügen des HDB-Benutzerspeicherschlüssels, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen.
- 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 dem SID-Adm-Benutzer konfigurieren. Für HANA-Systeme mit A22 als SID muss beispielsweise der HDB User Store Key mit a22adm konfiguriert

werden.

- Das SnapCenter Plug-in für SAP HANA Database unterstützt nicht das automatische Auffinden der Ressourcen in virtuellen RDM/VMDK-Umgebungen. Sie müssen Storage-Informationen für virtuelle Umgebungen bereitstellen und gleichzeitig Datenbanken manuell hinzufügen.

Über diese Aufgabe

Nach der Installation des Plug-ins werden alle Ressourcen auf diesem Linux-Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Die automatisch ermittelten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für SAP HANA aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen den Ressourcentyp aus der Liste Ansicht 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 zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, wird in der Spalte Status insgesamt nicht geschützt angezeigt.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn kein Backup-Vorgang durchgeführt wird, wird in der Spalte Gesamtstatus der Eintrag Backup Not Run angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

Wenn in der SAP HANA-Datenbank kein HDB-sicherer Benutzerspeicherschlüssel konfiguriert ist, wird neben der Ressource ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.

Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Nachdem Sie fertig sind

Sie müssen den HDB Secure User Store Key und den HDBSQL OS User so konfigurieren, dass sie die Datenbank schützen oder zur Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

Mandantenfähige Datenbank-Container werden für die Datensicherung vorbereitet

Bei direkt in SnapCenter registrierten SAP HANA Hosts wird das Installieren oder

Upgrade des SnapCenter Plug-ins für SAP HANA Database eine automatische Ermittlung der Ressourcen auf dem Host auslösen. Nach der Installation oder dem Upgrade des Plug-ins werden für alle MDC-Ressourcen (Multi-Tenant-Datenbank-Container), 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`“.

Über diese Aufgabe

Wenn sich beispielsweise in SnapCenter 4.2 die 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 Backups, die mit der Ressource von SnapCenter 4.2 und älteren Versionen verbunden sind, müssen bis zum Ablauf der Aufbewahrungsfrist aufbewahrt werden. Nach Ablauf des Aufbewahrungszeitraums können Sie die alte MDC-Ressource löschen und die neue automatisch erkannte MDC-Ressource weiterhin verwalten.

`Old MDC resource` Ist die MDC-Ressource für einen Plug-in-Host, der manuell in SnapCenter 4.2 oder früheren Versionen hinzugefügt wurde.

Führen Sie die folgenden Schritte durch, um die in SnapCenter 4.3 entdeckte neue Ressource für Datensicherungsvorgänge zu verwenden:

Schritte

1. Wählen Sie auf der Seite „Ressourcen“ die alte MDC-Ressource mit Backups aus, die der früheren SnapCenter-Version hinzugefügt wurden, und legen Sie sie auf der Topologieseite in den „`maintBuße-Modus`“.

   Wenn die Ressource Teil einer Ressourcengruppe ist, legen Sie die Ressourcengruppe in den „`mBetriebszustand`“.

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 erkannt wurde, nachdem der SnapCenter-Server und der Plug-in-Host auf 4.3 aktualisiert wurden. Die neue MDC-Ressource kann als Ressource mit demselben SID wie die alte MDC-Ressource, für einen bestimmten Host und mit einem roten Vorhängeschloss-Symbol daneben auf der Seite Ressourcen 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 Backups, die in SnapCenter 4.2 oder früheren Versionen basierend auf den Aufbewahrungseinstellungen erstellt wurden.
5. Löschen Sie die Ressourcengruppe auf der Seite Topologie.
6. Löschen Sie die alte MDC-Ressource von der Seite Ressourcen.

   Wenn die primäre Snapshot-Aufbewahrungsfrist beispielsweise 7 Tage beträgt und die Aufbewahrung sekundärer Snapshots 45 Tage beträgt, müssen Sie nach Abschluss von 45 Tagen und nach dem Löschen aller Backups die Ressourcengruppe und die alte MDC-Ressource löschen.

Verwandte Informationen

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

"Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an"

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

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 Systemreplizierung wird empfohlen, alle Ressourcen dieses HANA-Systems in eine Ressourcengruppe hinzuzufügen und ein Ressourcengruppenbackup durchzuführen. So wird für ein nahtloses Backup im Takeover-Failback-Modus gesorgt.

"Erstellen von Ressourcengruppen und Anhängen von Richtlinien".

Über diese Aufgabe

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

> Falls die oben genannten Ressourcen ermittelt werden, werden die Datensicherungsvorgänge von diesen Ressourcen nicht unterstützt.

- HANA Konfiguration für mehrere Hosts
- Mehrere Instanzen auf demselben Host
- Mehrschichtige Scale-out HANA System Replication
- Kaskadierte Replikationsumgebung im System Replication-Modus

Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter-Plug-in für 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 bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Ressourcentyp	Geben Sie den Ressourcentyp ein. Ressourcentypen sind Single-Container, Multitenant Database Container (MDC) und Non-Data-Volume.

Für dieses Feld…	Tun Sie das…
HANA-Systemname	Geben Sie den beschreibenden SAP HANA-Systemnamen ein. Diese Option ist nur verfügbar, wenn Sie einzelne Container- oder MDC-Ressourcentypen ausgewählt haben.
SID	Geben Sie die System-ID (SID) ein. Das installierte SAP HANA System wird durch eine einzige SID identifiziert.
Plug-in-Host	Wählen Sie den Plug-in-Host aus.
HDB Secure User Store Keys	Geben Sie den Schlüssel für die Verbindung zum SAP HANA-System ein. Der Schlüssel enthält die Anmeldeinformationen, um eine Verbindung zur Datenbank herzustellen. Für SAP HANA System Replication ist der sekundäre Benutzerschlüssel nicht validiert. Dies wird während der Übernahme verwendet.
HDBSQL OS-Benutzer	Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist. Für Windows ist es erforderlich, dass der HDBSQL OS-Benutzer der SYSTEMBENUTZER ist. Daher müssen Sie den HDB Secure User Store Key für den SYSTEMBENUTZER konfigurieren.

4. Wählen Sie auf der Seite Speicher-Footprint angeben ein Speichersystem aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Speichern**.

   Optional: Sie können auf das * -Symbol klicken  , um weitere Volumes, LUNs und qtrees von anderen Storage-Systemen hinzuzufügen.

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

   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 den Benutzern die Ressourcen zuweisen. Auf diese Weise 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 dem Hinzufügen der Datenbanken können Sie die Details der SAP HANA-Datenbank ändern.

Folgendes kann nicht geändert werden, wenn mit der SAP HANA-Ressource Backups verknüpft sind:

- Mandantenfähige Datenbank-Container (MDC): SID- oder HDBSQL Client (Plug-in)-Host
- Einzelner Container: SID- oder HDBSQL-Client (Plug-in)-Host
- Kein Datenvolumen: Ressourcenname, zugehöriger SID oder Plug-in-Host

Backup-Richtlinien für SAP HANA Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden, müssen Sie eine Backup-Richtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen zur Definition einer Datensicherungsstrategie für SAP HANA Datenbanken finden Sie in den Informationen.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das Hinzufügen von Ressourcen ausführen.
- Der SnapCenter Administrator muss Ihnen die SVMs sowohl für die Quell- als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren.

  Außerdem können Sie in der Richtlinie Replizierungs-, Skript- und Applikationseinstellungen festlegen. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

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

Über diese Aufgabe

- SAP HANA System Replication
  - Das primäre SAP HANA System ist gesichert, und alle Datensicherungsvorgänge können durchgeführt werden.
  - Sie können das sekundäre SAP HANA System schützen, aber die Backups können nicht erstellt werden.

    Nach dem Failover kann der gesamte Datensicherungsvorgang durchgeführt werden, wenn das sekundäre SAP HANA System zum primären SAP HANA System wird.

  Sie können kein Backup für SAP HANA Daten-Volume erstellen, aber SnapCenter schützt weiterhin die nicht-Daten-Volumes (NDV).

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Wenn Sie eine Snapshot-Sperrfrist festlegen, wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.

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

Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritte

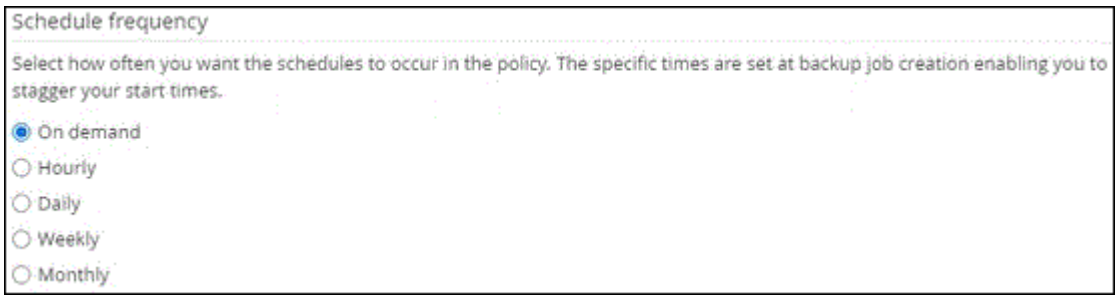
1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Einstellungen die folgenden Schritte aus:

◦ Wählen Sie den Sicherungstyp:

Ihr Ziel ist	Tun Sie das…
Führen Sie eine Integritätsprüfung der Datenbank durch	Wählen Sie * File-Based Backup* Aus. Es werden nur aktive Mandanten gesichert.
Erstellen Sie ein Backup mit Snapshot Technologie	Wählen Sie **Snapshot-Basiert** Aus.

◦ Geben Sie den Terminplantyp an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien und Backup-Häufigkeit verwenden, aber auch die Möglichkeit haben, den einzelnen Richtlinien unterschiedliche Backup-Zeitpläne zuzuweisen.



Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

◦ Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.

6. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Total Snapshot Copies to keep** aus, und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Wenn Sie Snapshot Backups auf Basis von Kopien aktivieren SnapVault möchten, müssen Sie die Aufbewahrungsanzahl auf 2 oder höher festlegen. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird. Für die SAP HANA-Systemreplizierung wird empfohlen, alle Ressourcen des SAP HANA-Systems in einer Ressourcengruppe hinzuzufügen. So wird sichergestellt, dass die richtige Anzahl von Backups beibehalten wird.

Ihr Ziel ist	Dann…
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Snapshot-Kopien behalten für**, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots vor dem Löschen behalten möchten.
Sperrfrist von Snapshot-Kopien	Wählen Sie die Sperrfrist für Snapshot Kopien aus und wählen Sie Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

7. Geben Sie für Snapshot-Copy-basierte Backups die Replikationseinstellungen auf der Seite Replikation an:

SAP HANA System Replication und sekundären SAP HANA System Replication auf 7 festgelegt. Sie können maximal 7 Snapshots

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Diese Option sollte für SnapMirror Active Sync aktiviert sein. Wenn die Sicherungsbeziehung in ONTAP vom Typ „Mirror and Vault“ ist und Sie nur diese Option auswählen, wird der auf dem primären Volume erstellte Snapshot nicht an das Zielsystem übertragen, sondern im Zielsystem aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt ist, um einen Wiederherstellungsvorgang durchzuführen, wird die Fehlermeldung „sekundärer Speicherort“ für die ausgewählte vaulted/mirrored Backup nicht verfügbar angezeigt. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Siehe "Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an".

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert. Weitere Informationen zu SnapLock Vault finden Sie unter "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel" Siehe "Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an".
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Anzahl der Wiederholversuche	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Über diese Aufgabe

- Zur Erstellung von SAP HANA System-Replikations-Backups wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. So wird für ein nahtloses Backup im Takeover-Failback-Modus gesorgt.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- 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-Status 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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

Für dieses Feld…	Tun Sie das…
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der Snapshot-Vorgang der Konsistenzgruppe abgeschlossen ist	Wählen Sie **dringend**, **Mittel** oder **entspannt** aus, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+

a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die Pre- und Post-Befehle für Stilllegung, Snapshot und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die für alle Datenschutzvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
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 Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüsselwerterpaare werden für SAP HANA Linux-Plug-in-Systeme unterstützt und nicht für SAP HANA-Datenbanken unterstützt, die als zentrales Windows-Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot Copy Tool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu verwenden und das Filesystem vor dem Erstellen eines Snapshots in einen konsistenten Zustand zu versetzen. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus. Diese Option ist für das SnapCenter-Plug-in für SAP HANA Database nicht verfügbar.
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** 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 Dropdown-Liste aus.

Sie können eine Richtlinie auch 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 Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

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

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

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

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

Erstellen einer Storage-Systemverbindung und einer Zertifizierung mit PowerShell cmdlets für SAP HANA Datenbank

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um SAP HANA Datenbanken zu sichern, wiederherzustellen oder zu klonen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mit dem Cmdlet Open-SmConnection.

```
PS C:\> Open-SmStorageConnection
```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel wird das Erstellen einer neuen Anmeldeinformationen namens FinanceAdmin mit Windows-Anmeldeinformationen angezeigt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Fügen Sie den SAP HANA-Kommunikationshost dem 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 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"}
```

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

SAP HANA Datenbanken sichern

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

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Stellen Sie für einen Backup-Vorgang mit Snapshot Kopie sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Zur Erstellung von SAP HANA System-Replikations-Backups wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. So wird für ein nahtloses Backup im Takeover-Failback-Modus gesorgt.

  "Erstellen von Ressourcengruppen und Anhängen von Richtlinien".

  "Sichern von Ressourcengruppen"

- Wenn Sie ein dateibasiertes Backup erstellen möchten, wenn eine oder mehrere Tenant-Datenbanken ausgefallen sind, setzen Sie den Parameter ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT in der HANA-Eigenschaftendatei mit Cmdlet auf **YES** `Set-SmConfigSettings` .

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

- Für Pre- und Post-Befehle für Stilllegung-, Snapshot- und Stilllegung-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host über die folgenden Pfade verfügbar sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

UI von SnapCenter

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ansicht** nach Ressourcentyp.

   Wählen Sie , und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um das Filterfenster zu schließen.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Seite Ressource **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.
5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   - Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der „Consistency Group Snapshot“-Vorgang abgeschlossen ist	Wählen Sie **dringend**, oder **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   - Wählen Sie den Pfeil von **Scripts** aus, um Pre- und Post-Befehle für Stilllegung-, Snapshot- und Unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

   - Wählen Sie den Pfeil **Custom Configurations**, und geben Sie dann die für alle Jobs, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.
   - Wählen Sie den Pfeil **Snapshot Copy Tool** aus, um das Werkzeug zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter zum Verwenden des Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen eines Snapshots einzugeben	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um einen Snapshot zu erstellen.

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

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

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

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

   b. Wählen Sie * * + in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

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

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

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

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

    b. Wählen Sie **Backup**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
    - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

      Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der 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 auf Folgendes: *Java -jar -Xmx8192M -Xms4096M*

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-smconnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Mit dem Cmdlet "Add-SmResources" können Sie Ressourcen hinzufügen.

   Dieses Beispiel zeigt, wie eine SAP HANA-Datenbank des SingleContainer-Typs hinzugefügt wird:

```
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_'
```

In diesem Beispiel wird das Hinzufügen einer SAP HANA-Datenbank mit MultipleContainers-Typ beschrieben:

```
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 Sie eine Ressource erstellen, die nicht auf dem Datenvolumen ist:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   In diesem Beispiel wird eine Backup-Richtlinie für ein auf Snapshot Kopien basierendes Backup erstellt:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
   Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
   ```

   In diesem Beispiel wird eine Backup-Richtlinie für ein dateibasiertes Backup erstellt:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
   -PluginPolicyType hana -BackupType FileBasedBackup
   ```

4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.

   Dieses Beispiel schützt eine einzelne Container-Ressource:

```
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.sccore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Dieses Beispiel erstellt eine Ressourcengruppe ohne Daten-Volume:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

Dieses Beispiel sichert eine geschützte Ressource:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Überwachen Sie den Job-Status (ausgeführt, abgeschlossen oder fehlgeschlagen) mit dem Cmdlet "Get-smJobSummaryReport".

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Überwachen Sie die Details zu Backup-Jobs wie Backup-ID, Backup-Name zum Wiederherstellen oder Klonen mit dem Cmdlet "Get-SmBackupReport".

```
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 :
```

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

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Über diese Aufgabe

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie , auswählen und dann das Tag auswählen. Sie können dann auswählen , um das Filterfenster 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Monitoring von Backup-Vorgängen bei SAP HANA Datenbanken

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

Überwachen von Datensicherungsvorgängen in SAP HANA-Datenbanken im Bereich „Activity“

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

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

Schritte

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

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

Abbrechen der Backup-Vorgänge für SAP HANA

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *, um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

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

sind.

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

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

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

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

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

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

Schritte

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

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

4. Lesen Sie die **Übersichtskarte** durch, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

Im Abschnitt **Summary Card** wird die Gesamtzahl der dateibasierten Backups, auf Snapshot-Kopien basierenden Backups und Clones angezeigt.

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

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

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

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

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

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

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

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

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

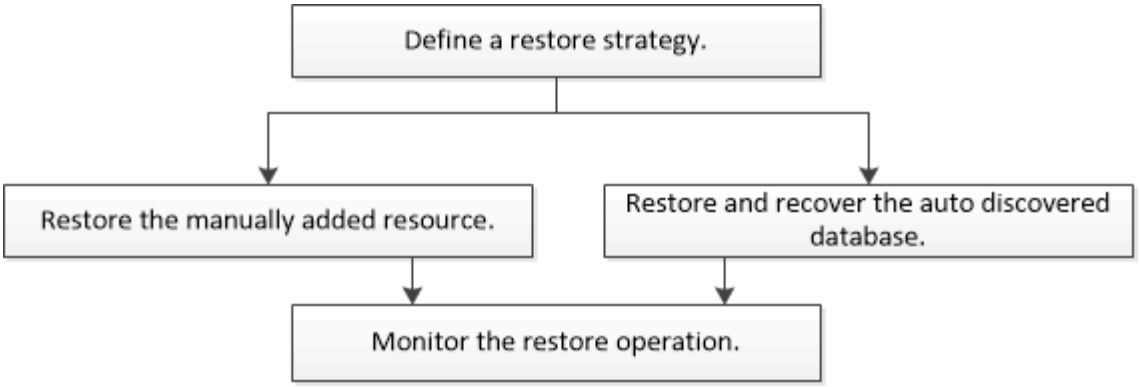
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

Wiederherstellung von SAP HANA Datenbanken

Wiederherstellung des Workflows

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

"SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Dateibasierte Backup-Kopien können nicht aus SnapCenter wiederhergestellt werden.
- Nach einem Upgrade auf SnapCenter 4.3 können die in SnapCenter 4.2 erstellten Backups wiederhergestellt werden, können aber nicht wiederhergestellt werden. Zur Wiederherstellung der in SnapCenter 4.2 erstellten Backups muss HANA Studio oder HANA-Recovery-Skripte außerhalb von SnapCenter verwendet werden.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

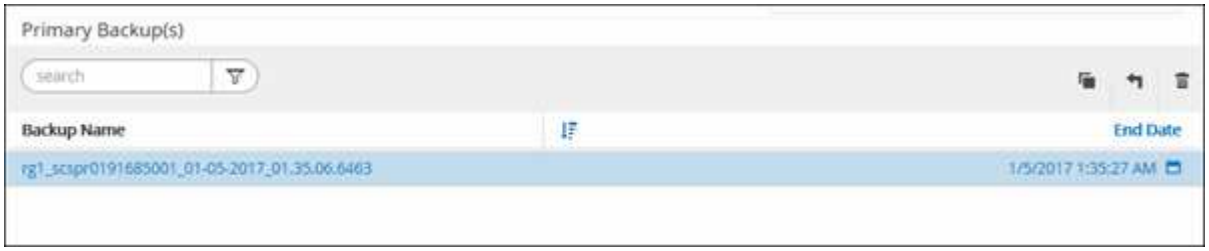
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite „Bereich wiederherstellen“ die Option **vollständige Ressource** oder **Dateiebene** aus.

   a. Wenn Sie **Complete Resource** auswählen, werden alle konfigurierten Datenvolumen der SAP HANA Datenbank wiederhergestellt.

      Wenn die Ressource Volumes oder qtrees enthält, werden die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf denselben Volumes oder qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

   b. Wenn Sie **File Level** auswählen, können Sie entweder **Alle** auswählen oder die spezifischen Volumes oder qtrees auswählen und dann den Pfad eingeben, der mit diesen Volumes oder qtrees verbunden ist, 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 vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

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

Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.

- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Dateibasierte Backup-Kopien können nicht aus SnapCenter wiederhergestellt werden.
- Nach einem Upgrade auf SnapCenter 4.3 können die in SnapCenter 4.2 erstellten Backups wiederhergestellt werden, können aber nicht wiederhergestellt werden. Zur Wiederherstellung der in SnapCenter 4.2 erstellten Backups muss HANA Studio oder HANA-Recovery-Skripte außerhalb von SnapCenter verwendet werden.
- Bei ONTAP 9.12.1 und älteren Versionen übernehmen die durch die SnapLock Vault Snapshots im Rahmen der Wiederherstellung erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Filtern Sie auf der Seite Ressourcen die Ressourcen aus der Dropdown-Liste **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

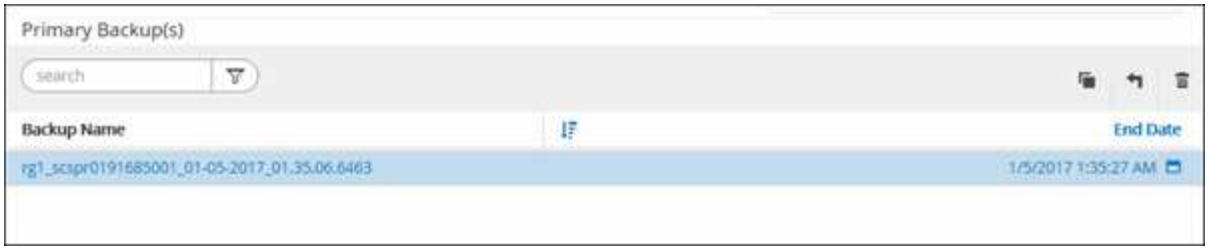
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * *  .



6. Wählen Sie auf der Seite Restore Scope die Option **Complete Resource** aus, um die konfigurierten Datenvolumen der SAP HANA-Datenbank wiederherzustellen.

   Sie können entweder **Complete Resource** (mit oder ohne **Volume revert**) oder **Tenant Database** auswählen.

   Der Wiederherstellungsvorgang wird von SnapCenter Server für mehrere Mandanten nicht unterstützt, wenn der Benutzer entweder die Option **Tenant Database** oder **Complete Restore** wählt. Sie müssen HANA Studio oder HANA Python Script verwenden, um die Wiederherstellung durchzuführen.

   a. Wählen Sie **Volume revert** aus, wenn Sie das gesamte Volume wiederherstellen möchten.

      Diese Option steht für Backups zur Verfügung, die in SnapCenter 4.3 in NFS-Umgebungen erstellt wurden.

      Wenn die Ressource Volumes oder qtrees enthält, werden die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht. Dies gilt, wenn die Option **Complete Resource** mit **Volume revert** zur Wiederherstellung ausgewählt ist.

   b. Wählen Sie **Tenant Database**.

      Diese Option ist nur für MDC-Ressourcen verfügbar.

      Stellen Sie sicher, dass die Mandantendatenbank angehalten wird, bevor Sie den Wiederherstellungsvorgang ausführen.

   Wenn Sie die Option **Tenant Database** wählen, müssen Sie HANA Studio verwenden oder HANA Recovery Scripts außerhalb von SnapCenter verwenden, um den Recovery-Vorgang durchzuführen.

7. Wählen Sie auf der Seite Recovery Scope eine der folgenden Optionen aus:

Sie suchen…	Tun Sie das…
Möchten so nah wie möglich bis zur aktuellen Zeit wiederherstellen	Wählen Sie **Wiederherstellen in aktuellster Zustand**. Bei einzelnen Container-Ressourcen legen Sie einen oder mehrere Backup-Standorte für Protokolle und Kataloge fest. Bei mandantenfähigen Datenbank-Containern (MDC) müssen ein oder mehrere Log-Backup-Standorte und der Backup-Katalog-Speicherort angegeben werden. Bei MDC-Ressourcen sollte der Pfad sowohl Systemdatenbank- als auch Mandantendatenbankprotokolle enthalten.

Sie suchen…	Tun Sie das…
Wiederherstellung auf den angegebenen Zeitpunkt	Wählen Sie **Wiederherstellen zu Zeitpunkt**. a. Wählen Sie die Zeitzone aus. Die Browser-Zeitzone wird standardmäßig ausgefüllt. Die ausgewählte Zeitzone wird zusammen mit der Eingangszeit in absolute GMT umgewandelt. b. Geben Sie Datum und Uhrzeit ein. Beispielsweise befindet sich der HANA Linux-Host in Sunnyvale, Kalifornien, und der Benutzer in Raleigh, North Carolina, USA, stellt die Anmeldung bei SnapCenter wieder bereit. Der Zeitunterschied zwischen diesen beiden Speicherorten beträgt 3 Stunden. Da sich der Benutzer in Raleigh, North Carolina, angemeldet hat, ist die Standardzeitzone für den Browser, die in der Benutzeroberfläche ausgewählt wird, GMT-04:00. Wenn der Benutzer eine Wiederherstellung auf 5 a.m .Sunnyvale, CA durchführen möchte, dann muss der Benutzer die Browser-Zeitzone auf die HANA Linux Host Zeitzone einstellen, die GMT-07:00 ist und das Datum und die Zeit als 5:00 Uhr angeben Bei einzelnen Container-Ressourcen legen Sie einen oder mehrere Backup-Standorte für Protokolle und Kataloge fest. Geben Sie bei MDC-Ressourcen einen oder mehrere Backup-Speicherorte und den Speicherort des Backup-Katalogs an. Bei MDC-Ressourcen sollte der Pfad sowohl Systemdatenbank- als auch Mandantendatenbankprotokolle enthalten.
Recovery für ein bestimmtes Daten-Backup erforderlich	Wählen Sie **Wiederherstellen in spezifizierter Datensicherung**.
Möchten Sie nicht wiederherstellen	Wählen Sie **Keine Wiederherstellung**. Sie müssen den Recovery-Vorgang manuell aus dem HANA Studio durchführen.

Sie können nur die Backups wiederherstellen, die nach einem Upgrade auf SnapCenter 4.3 erstellt

wurden, sofern sowohl der Host als auch das Plug-in auf SnapCenter 4.3 aktualisiert werden. Die für die Wiederherstellung ausgewählten Backups werden nach der Konvertierung der Ressource oder der Entdeckung als automatisch erkannte Ressource erstellt.

8. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

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

    Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   PS C:\> Open-Smconnection
   ```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

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

Überwachen von Restore-Vorgängen bei SAP HANA Datenbanken

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

Über diese Aufgabe

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

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

-  In Bearbeitung

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

Schritte

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

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

Backups von SAP HANA Ressourcen klonen

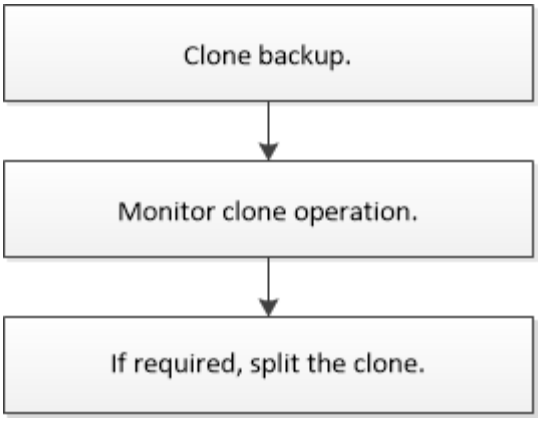
Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

- Sie können auf dem SAP HANA-Quellserver klonen.
- Sie können Ressourcen-Backups aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses
  - Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

Klonen eines Backups einer SAP HANA Datenbank

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen.

Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Sie können keine dateibasierten Backups klonen.
- Der Ziel-Klon-Server sollte dieselbe SAP HANA-Instanz-SID haben, die im Feld Ziel-Klon-SID bereitgestellt wird.
- Wenn Sie Befehle vor dem Klonen oder nach dem Klonen ausführen, sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host über folgende Pfade vorhanden sind:
  - Für Windows: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Für Linux: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*

Wenn die Befehle in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Bei ONTAP 9.12.1 und älteren Versionen übernehmen die aus den SnapLock Vault Snapshots im Rahmen der Wiederherstellung erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugeordnete 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 Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Plug-in-Host	Wählen Sie den Host aus, auf dem der Klon gemountet werden soll, und das Plug-in ist installiert.
Ziel Klon-SID	Geben Sie die SAP HANA Instanz-ID ein, die aus den vorhandenen Backups geklont werden soll.
NFS-Export-IP-Adresse	Geben Sie IP-Adressen oder Hostnamen ein, auf denen die geklonten Volumes exportiert werden.
ISCSI-Initiator	Geben Sie den iSCSI-Initiatornamen des Hosts ein, an den die LUNs exportiert werden. Diese Option ist nur verfügbar, wenn Sie den Ressourcentyp LUN ausgewählt haben.
Protokoll	Geben Sie das LUN-Protokoll ein. Diese Option ist nur verfügbar, wenn Sie den Ressourcentyp LUN ausgewählt haben.

Wenn die ausgewählte Ressource eine LUN ist und Sie aus einem sekundären Backup klonen, werden die Ziel-Volumes aufgelistet. Es können mehrere Ziel-Volumes an einer einzigen Quelle vorhanden sein.

Vor dem Klonen müssen Sie sicherstellen, dass der iSCSI-Initiator oder das FCP vorhanden ist und bei alternativen Hosts konfiguriert und angemeldet sind.

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 den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
      - Befehl Pre Clone: Löschen Sie vorhandene Datenbanken mit demselben Namen
      - Befehl nach Clone: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.
   b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

      Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:

   Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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

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

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

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Rufen Sie die Backups für den Klonvorgang mit dem Cmdlet Get-SmBackup ab.

   Dieses Beispiel zeigt, dass zwei Backups 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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

   Dieses Beispiel zeigt, dass für das zu klonendes Backup eine NFSExportIPs-Adresse von 10.232.206.169 vorhanden ist:

```
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 sind, wird der Standardwert auf den Klon-Zielhost exportiert.

4. Überprüfen Sie, ob die Backups erfolgreich geklont wurden, indem Sie das Cmdlet "Get-SmCloneReport" verwenden, um die Details zu den Klonjobs anzuzeigen.

   Sie können Details wie Klon-ID, Startdatum und -Zeit, Enddatum und -Zeit 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          :
```

Überwachung von Klonvorgängen für SAP HANA Datenbanken

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

Über diese Aufgabe

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

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

Schritte

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

Teilen Sie einen Klon auf

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

Über diese Aufgabe

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

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

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

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

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

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

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

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

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

   Beispiel:

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

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

Verwandte Informationen

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

Löschen oder teilen Sie SAP HANA Datenbankklone nach dem Upgrade der SnapCenter

Nach einem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource, aus der die Klone erstellt wurden, aufteilen.

Über diese Aufgabe

Wenn Sie den Storage-Footprint der verborgenen Klone ermitteln möchten, führen Sie den folgenden Befehl aus: `Get-SmClone -ListStorageFootprint`

Schritte

1. Löschen Sie die Backups der geklonten Ressourcen mit dem Cmdlet "remove-smbackup".
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mit dem Cmdlet "remove-sresourcgruppe".
3. Entfernen Sie den Schutz der geklonten Ressource mit dem Cmdlet "remove-smprotectResource".
4. Wählen Sie auf der Seite Ressourcen die übergeordnete Ressource aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht Kopien managen die Klone entweder auf den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen 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**.

Schutz von Oracle Datenbanken

Überblick über das SnapCenter Plug-in für Oracle Database

Welche Möglichkeiten bietet das Plug-in für Oracle Database

Das SnapCenter Plug-in für Oracle Database ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das applikationsspezifische Datensicherungsmanagement von Oracle Datenbanken ermöglicht.

Das Plug-in für Oracle Database automatisiert das Backup, die Katalogisierung und die Katalogisierung mit Oracle Recovery Manager (RMAN), Überprüfung, Mounten, Unmounten, Restore, Recovery und Klonen von Oracle Datenbanken in Ihrer SnapCenter Umgebung. Das Plug-in für Oracle Database installiert das SnapCenter Plug-in für UNIX, um alle Datensicherungsvorgänge auszuführen.

Sie können mit dem Plug-in für Oracle Database Backups von Oracle Datenbanken, auf denen SAP Applikationen ausgeführt werden, verwalten. Die Integration von SAP BR*Tools wird jedoch nicht unterstützt.

- Sichern Sie Datendateien, Kontrolldateien und Archivprotokolldateien.

  Backup wird nur auf CDB-Ebene (Container-Datenbank) unterstützt.

- Wiederherstellung und Recovery von Datenbanken, Datenbanken und Plug-in-Datenbanken (PDBs).

  Unvollständige Wiederherstellung von PDBs wird nicht unterstützt.

- Erstellung von Klonen von Produktionsdatenbanken bis zu einem bestimmten Zeitpunkt

  Das Klonen wird nur auf CDB-Ebene unterstützt.

- Sofortige Überprüfung der Backups.
- Mounten und Aufheben von Daten und Protokollierung von Backups für den Wiederherstellungsvorgang.
- Planung von Backup- und Verifizierungsvorgängen
- Monitoring aller Vorgänge
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

Funktionen von Plug-in für Oracle Database

Das Plug-in für Oracle Database ist in die Oracle Datenbank auf dem Linux oder AIX Host und in NetApp Technologien auf dem Storage-System integriert.

- Einheitliche grafische Benutzeroberfläche

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore-, Recovery- und Klonvorgänge über alle Plug-ins hinweg, zentralisierte Berichterstellung, Dashboard-Ansichten auf einen Blick, rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Aufgaben über alle Plug-ins hinweg.

- Automatisierte, zentrale Administration

Sie können Backup- und Klonvorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- Unterbrechungsfreie NetApp Snapshot Technologie

  SnapCenter verwendet NetApp Snapshot Technologie mit dem Plug-in für Oracle Database und dem Plug-in für UNIX, um Datenbanken zu sichern. Snapshots belegen nur minimalen Speicherplatz.

Das Plug-in für Oracle Database bietet darüber hinaus folgende Vorteile:

- Unterstützung für Backup, Restore, Klonen, Mounten, Unmounten, Und Verifizierungs-Workflows
- Automatische Erkennung von auf dem Host konfigurierten Oracle-Datenbanken
- Unterstützung von Katalogisierung und Katalogisierung mit Oracle Recovery Manager (RMAN)
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Unterstützung von Archive Log Management (ALM) für Restore- und Klonvorgänge
- Erstellung platzsparender und zeitpunktgenauer Kopien von Produktionsdatenbanken für Test- oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Die Unterstützung der Konsistenzgruppendaten (CG) von ONTAP im Rahmen der Erstellung von Backups in SAN- und ASM-Umgebungen
- Unterbrechungsfreie und automatisierte Backup-Verifizierung
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Datenbank-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Datenbanken in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Unterstützung physischer und virtualisierter Infrastrukturen
- Unterstützung von NFS, iSCSI, Fibre Channel (FC), RDM, VMDK über NFS und VMFS sowie ASM over NFS, SAN, RDM und VMDK
- Unterstützung für die Selective LUN Map (SLM)-Funktion von ONTAP

  Standardmäßig erkennt die SLM-Funktion regelmäßig die LUNs, die keine optimierten Pfade haben, und behebt sie. 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 FÜR DEN PARAMETER ENABLE_LUNPATH_MONITORING auf false setzen.
  - Sie können die Häufigkeit angeben, in der die LUN-Pfade automatisch korrigiert werden, indem Sie den Wert (in Stunden) dem Parameter „LUNPATH_MONITORING_INTERVAL“ zuweisen. Informationen zu SLM finden Sie im "ONTAP 9 – Systemadministrationshandbuch".

- Unterstützung für Non-Volatile Memory Express (NVMe) unter Linux

  - NVMe util sollte auf dem Host installiert werden.

Sie müssen NVMe util installieren, um auf einem alternativen Host zu klonen oder einzubinden.

- Backup, Wiederherstellung, Klonen, mounten, unmounten, Katalogvorgänge, Unkatalogs und Verifizierungen werden auf der NVMe Hardware unterstützt, ausgenommen die virtualisierten Umgebungen wie RDM.

  Die oben genannten Operationen werden auf Geräten ohne Partitionen oder mit einer einzigen Partition unterstützt.

  Sie können Multipathing-Lösung für NVMe-Geräte konfigurieren, indem Sie die native Multipathing-Option im Kernel einstellen. Multipathing von Device Mapper (DM) wird nicht unterstützt.

- Backup, Wiederherstellung, Klonen, mounten, unmounten, Katalog-, Unkatalogs- und Verifizierungsworkflows werden auf NVMe over TCP/IP unterstützt.
- Backup, Wiederherstellung, Klonen, mounten, unmounten, Katalog-, Unkatalogs- und Verifizierungsworkflows werden auf VMDK-Layout unterstützt, das auf NVMe over TCP/IP erstellt wurde.

- Unterstützung von SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Business Services auch bei einem vollständigen Standortausfall weiterlaufen können und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.
- Unterstützt alle nicht standardmäßigen Benutzer anstelle von oracle und Grid.

  Um die nicht-default-Benutzer zu unterstützen, sollten Sie die nicht-default-Benutzer einstellen, indem Sie die Werte der Parameter in der Datei **sco.properties** unter *file /var/opt/snapcenter/sco/etc/* ändern.

  Die Standardwerte der Parameter werden als oracle und Grid festgelegt.

  - DB_USER=oracle
  - DB_GROUP=oinstall
  - GI_USER=Grid
  - GI_GROUP=oinstall

Von Plug-in für Oracle Database unterstützte Storage-Typen

SnapCenter unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf Virtual Machines. Sie müssen die Unterstützung Ihres Speichertyps überprüfen, bevor Sie das SnapCenter Plug-ins Paket für Linux oder SnapCenter Plug-ins Package für AIX installieren.

SnapCenter unterstützt Storage-Bereitstellung für Linux und AIX nicht.

Storage-Typen unterstützt auf Linux

In der folgenden Tabelle sind die unter Linux unterstützten Speichertypen aufgeführt.

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung • NVMe-FC • NVMe/TCP
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datastores • VMDKs auf VMFS, die über NVMe/TCP erstellt wurden ⓘ RAC wird auf ESX 8.0U2 unterstützt, das die Unterstützung für gemeinsam genutzte VMDK hat • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Storage Types supported auf AIX

In der folgenden Tabelle sind die auf AIX unterstützten Storage-Typen aufgeführt.

Maschine	Storage-Typ
Physischer Server	• FC-connected und iSCSI-Connected LUNs. In einer SAN-Umgebung werden ASM, LVM und SAN-Dateisysteme unterstützt. NFS auf AIX und Dateisystem wird nicht unterstützt. • Erweitertes Journaled File System (JFS2) Unterstützt die Inline-Protokollierung auf SAN-Dateisystemen und LVM-Layout.

Das "NetApp Interoperabilitäts-Matrix-Tool" enthält die neuesten Informationen zu den unterstützten Versionen.

Storage-Systeme für SnapMirror und SnapVault Replizierung für Plug-in für Oracle vorbereiten

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Minimale ONTAP-Berechtigungen, die für das Plug-in für Oracle erforderlich sind

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-

ins, die Sie zur Datensicherung verwenden.

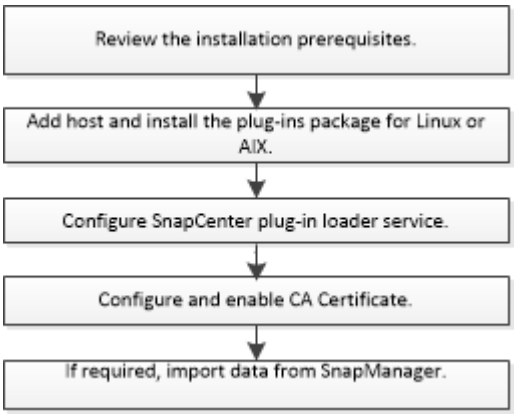
- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun-Attribut anzeigen
  - lun erstellen
  - lun löschen
  - lun-Geometrie
  - lun Initiatorgruppe hinzufügen
  - lun-Initiatorgruppe wird erstellt
  - lun-Initiatorgruppe löschen
  - lun igroup umbenennen
  - lun-Initiatorgruppe wird angezeigt
  - lun Mapping Add-Reporting-Nodes
  - lun-Zuordnung erstellen
  - lun-Zuordnung löschen
  - lun Mapping remove-Reporting-Nodes
  - lun-Zuordnung wird angezeigt
  - lun ändern
  - lun-Verschiebung in Volume
  - lun ist offline
  - lun ist online
  - lun Persistent-Reservierung löschen
  - die lun-Größe wird geändert
  - lun seriell
  - lun anzeigen
  - SnapMirror Richtlinie Add-Rule
  - änderungsregel für snapmirror
  - Remove-Rule für snapmirror-Richtlinie
  - snapmirror-Richtlinie anzeigen
  - snapmirror Wiederherstellung
  - snapmirror zeigen
  - snapmirror Vorgeschichte
  - snapmirror Update
  - snapmirror Update-ls-Set

- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen
- Show-Disk-Nutzung für Volume-Dateien
- Volume ist offline
- Das Volume ist online
- Volume-Änderung
- Erstellen von Volume-qtree
- Volume qtree löschen
- Änderung des Volume-qtree
- Volume-qtree anzeigen
- Volume-Einschränkung
- Volumen anzeigen
- Erstellen von Volume-Snapshots
- Volume Snapshot löschen
- Ändern des Volume-Snapshots
- Umbenennung von Volume-Snapshots
- Wiederherstellung von Volume Snapshots
- Restore-Datei für Volume Snapshots
- Volume-Snapshot werden angezeigt
- Volume-Aufhängung nicht verfügbar
- vserver
- cifs von vserver
- vserver cifs shadowcopy anzeigen
- vserver zeigen
- Netzwerkschnittstelle
- Netzwerkschnittstelle wird angezeigt
- MetroCluster zeigen

Installieren Sie das SnapCenter Plug-in für Oracle Database

Installations-Workflow des SnapCenter Plug-ins für Oracle Database

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 von Plug-ins Package für Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-ins-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 Benutzer ohne Root 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 als effektiver nicht-Root-Benutzer ausgeführt.

- Wenn Sie das SnapCenter Plug-ins Paket für AIX auf 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, nicht aber die symbolischen Links auf Verzeichnisebene, um den ABSOLUTEN Pfad JAVA_HOME zu erhalten.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus als 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 Version VON JAVA 11 auf dem Linux-Host installiert haben.

- Für Oracle Datenbanken, die auf einem Linux oder AIX Host laufen, sollten Sie sowohl das SnapCenter Plug-in für Oracle Database als auch das SnapCenter Plug-in für UNIX installieren.

Sie können das Plug-in für Oracle Database auch zur Verwaltung von Oracle Datenbanken für SAP verwenden. Die Integration von SAP BR*Tools wird jedoch nicht unterstützt.

- Wenn Sie Oracle Database 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 Host-Anforderungen

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

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux Wenn Sie die Oracle-Datenbank auf LVM unter Oracle Linux oder Red hat Enterprise Linux 6.6 oder 7.0 verwenden, müssen Sie die neueste Version von Logical Volume Manager (LVM) installieren. • SUSE Linux Enterprise Server (SLES)
MindestRAM für das SnapCenter Plug-in auf dem Host	2GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

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

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

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter 2.0 und höheren Versionen kann ein nicht-Root-Benutzer das SnapCenter Plug-ins-Paket für Linux installieren und das Plug-in-Verfahren 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Stellen Sie für den Benutzer, der nicht root ist, sicher, dass der Name des Benutzers, der nicht root ist, und die Gruppe des Benutzers identisch sein sollten.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

AIX Host-Anforderungen

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

Das SnapCenter Plug-in für UNIX, das Teil des SnapCenter Plug-ins-Pakets für AIX ist, unterstützt keine gleichzeitigen Volume-Gruppen.

Element	Anforderungen
Betriebssysteme	AIX 7.1 oder höher
MindestRAM für das SnapCenter Plug-in auf dem Host	4GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	Java 11 IBM Java Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

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

Konfigurieren Sie sudo-Berechtigungen für Benutzer, die nicht root sind, für 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_Host_Plugin.bsx
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

AIX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Anmeldedaten einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten 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 Benutzer ohne Root-Benutzer erstellt, der über sudo-Berechtigungen zum Installieren und Starten des Plug-in-Prozesses verfügt.

Weitere Informationen finden Sie unter: Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts Oder die nicht root sind, für AIX-Host

Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten erstellen dürfen, empfiehlt es sich, erst nach dem Hinzufügen von SVMs Anmeldeinformationen zu erstellen, bevor Sie Hosts implementieren und Plug-ins installieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Anmeldeinformationen die Anmeldeinformationen ein:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domain-Administrator Geben Sie den Domänenadministrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username*

Für dieses Feld…	Tun Sie das…
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten. Wählen Sie je nach Betriebssystem des Plug-in-Hosts entweder Linux oder AIX aus.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite **Benutzer und Zugriff** die Pflege von Anmeldeinformationen zuweisen.

Konfigurieren von Anmeldeinformationen für eine Oracle-Datenbank

Sie müssen Anmeldedaten konfigurieren, die für Datensicherungsvorgänge 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 Anmeldedaten".

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername keine vollständigen Administratorrechte hat, muss der Benutzername mindestens über Ressourcengruppen- und Sicherungsrechte verfügen.

Wenn Sie die Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ansicht Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Sie müssen Datenbankanmeldeinformationen konfigurieren, um die Datenbank schützen oder zur Ressourcengruppe hinzufügen zu können, um Datensicherungsvorgänge durchzuführen.

Wenn Sie beim Erstellen einer Anmeldedaten falsche Details angeben, wird eine Fehlermeldung angezeigt. Klicken Sie auf **Abbrechen** und versuchen Sie es dann erneut.

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 Sie auf , und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern.

   Sie können dann klicken , 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 in der Dropdown-Liste **vorhandene Anmeldedaten verwenden** die Anmeldeinformationen aus, die zum Ausführen von Datensicherungsjobs in der Oracle-Datenbank verwendet werden sollen.

   Der Oracle-Benutzer sollte über sysdba-Berechtigungen verfügen.

   Sie können auch Anmeldeinformationen erstellen, indem Sie auf klicken .

6. Wählen Sie im Abschnitt ASM-Einstellungen konfigurieren in der Dropdown-Liste **vorhandene Anmeldedaten verwenden** die Anmeldeinformationen aus, die für die Ausführung von Datensicherungsjobs auf der ASM-Instanz verwendet werden sollen.

   Der ASM-Benutzer sollte über syssm-Berechtigung verfügen.

   Sie können auch Anmeldeinformationen erstellen, indem Sie auf klicken .

7. Wählen Sie im Abschnitt Configure RMAN Catalog Settings aus der Dropdown-Liste **Use Existing Credentials** die Anmeldeinformationen aus, die für die Ausführung von Datenschutzaufträgen in der Oracle Recovery Manager (RMAN)-Katalogdatenbank verwendet werden sollen.

   Sie können auch Anmeldeinformationen erstellen, indem Sie auf klicken .

   Geben Sie im Feld **TNSName** den Namen der TNS-Datei (Transparent Network Substrat) ein, der vom SnapCenter-Server zur Kommunikation mit der Datenbank verwendet wird.

8. Geben Sie im Feld **bevorzugte RAC-Knoten** die RAC-Knoten (Real Application Cluster) an, die für das Backup bevorzugt sind.

   Die bevorzugten Knoten sind möglicherweise ein oder alle Cluster-Knoten, wo die RAC-Datenbankinstanzen vorhanden sind. Der Backup-Vorgang wird nur auf den bevorzugten Knoten in der bevorzugten Reihenfolge ausgelöst.

   In RAC One Node wird nur ein Knoten in den bevorzugten Knoten aufgelistet, und dieser bevorzugte Knoten ist der Knoten, auf dem die Datenbank derzeit gehostet wird.

   Nach dem Failover oder der Verschiebung der RAC One Node-Datenbank wird durch die Aktualisierung von Ressourcen auf der Seite SnapCenter-Ressourcen der Host aus der Liste **bevorzugte RAC-Knoten** entfernt, in der die Datenbank zuvor gehostet wurde. Der RAC-Knoten, in dem die Datenbank verschoben wird, wird in **RAC-Knoten** aufgelistet 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 mithilfe der GUI das Plug-ins Package für Linux oder AIX

Auf der Seite „Host hinzufügen“ können Sie Hosts hinzufügen, und dann das SnapCenter Plug-ins Paket für Linux oder SnapCenter Plug-ins Package 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 für einen einzelnen Host oder für ein Cluster installieren. Wenn Sie das Plug-in auf einem Cluster installieren (Oracle RAC), 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.

Nur passwortbasierte Authentifizierung wird unterstützt, wenn Sie das Plug-in auf einem Oracle RAC installieren. Die auf SSH-Schlüssel basierende Authentifizierung wird nicht unterstützt.

Sie sollten einer Rolle zugewiesen werden, die über die Berechtigungen zum Installieren und Deinstallieren des Plug-ins verfügt, z. B. über die Rolle „SnapCenter Admin“.

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

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie als Hosttyp * Linux* oder **AIX** aus. 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.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Jeder Node in der Oracle Real Application Clusters (RAC)-Umgebung Knoten-VIP oder Scan-IP wird nicht unterstützt Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist */opt/NetApp/snapcenter*. Optional können Sie den Pfad anpassen.
Fügen Sie alle Hosts im Oracle RAC hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem Oracle RAC hinzuzufügen. In einem Flex ASM-Setup werden alle Knoten, unabhängig davon, ob es sich um einen Hub- oder Leaf-Knoten handelt, hinzugefügt.
Überspringen Sie optionale Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

7. Klicken Sie Auf **Absenden**.

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

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

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

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

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

In einer Cluster-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

SnapCenter unterstützt keinen ECDSA-Algorithmus.

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

9. Überwachen Sie den Installationsfortschritt.

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

Ergebnis

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

Überwachung des Installationsstatus

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

Über diese Aufgabe

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

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

Schritte

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

Alternative Möglichkeiten, Plug-ins Package für Linux oder AIX zu installieren

Sie können das Plug-ins-Paket für Linux oder AIX auch manuell installieren, indem Sie die Cmdlets oder CLIs verwenden.

Vor der manuellen Installation des Plug-ins sollten Sie die Signatur des Binärpakets mit dem Schlüssel **snapcenter_public_key.Pub** und **snapcenter_linux_Host_Plugin.bin.sig** validieren. Diese befinden sich unter *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Vergewissern Sie sich, dass **OpenSSL 1.0.2g** auf dem Host installiert ist, auf dem Sie das Plug-in installieren möchten.

Überprüfen Sie die Signatur des Binärpakets, indem Sie den 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_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

Installieren Sie sie mithilfe von Cmdlets auf mehreren Remote Hosts

Sie sollten das Cmdlet *Install-SmHostPackage* PowerShell 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 bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet sein.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das SnapCenter Plug-ins Paket für Linux oder SnapCenter Plug-ins Paket für AIX mit dem Cmdlet *Install-SmHostPackage* und den erforderlichen Parametern.

   Sie können die Option *-skipprecheck* 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 Precheck-Skript überprüft den Firewall-Status des Plug-in-Ports nicht, wenn er in den Regeln für die Ablehnung der Firewall angegeben ist.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

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

Installation auf Cluster-Host

Sie sollten SnapCenter Plug-ins Package für Linux oder SnapCenter Plug-ins Package für AIX auf beiden Knoten des Cluster-Hosts installieren.

Jeder der Nodes des Cluster-Hosts verfügt über 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 Package für Linux oder das SnapCenter Plug-ins Package für AIX auf beiden Knoten des Cluster-Hosts.
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 nicht in spl.properties angegeben ist, können Sie es hinzufügen und den Wert SCO,SCU zuordnen.

3. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, und geben Sie dann Ihre Anmeldeinformationen ein.
4. Legen Sie in jedem Knoten die bevorzugten IPs des Knotens mithilfe des Befehls *set-PreferredHostIPsInStorageExportPolicy* scli und der erforderlichen Parameter fest.
5. Fügen Sie im SnapCenter-Serverhost einen Eintrag für die Cluster-IP und den entsprechenden DNS-Namen in *C:\Windows\System32\drivers\etc\Hosts* hinzu.
6. Fügen Sie den Knoten mithilfe des 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 ein Backup der Datenbank. Wenn ein Failover auftritt, können Sie das auf Node 1 erstellte Backup verwenden, um die Datenbank auf Node 2 wiederherzustellen. Sie können auch das auf Node 1 erstellte Backup verwenden, um einen Klon auf Node 2 zu erstellen.

Es gibt veraltete Volumes, Verzeichnisse und Sperrdateien, wenn das Failover während der Ausführung anderer SnapCenter Vorgänge durchgeführt wird.

Installieren Sie das Plug-ins-Paket für Linux im Silent-Modus

Sie können das SnapCenter-Plug-ins-Paket für Linux im Silent-Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-ins-Pakets überprüfen.
- Sie sollten sicherstellen, dass die UMGEBUNGSVARIABLE DISPLAY nicht eingestellt ist.

  Wenn die UMGEBUNGSVARIABLE DISPLAY eingestellt ist, sollten Sie die Anzeige Unset ausführen und anschließend versuchen, das Plug-in manuell zu installieren.

Über diese Aufgabe

Bei der Installation im Konsolenmodus müssen Sie die erforderlichen Installationsinformationen bereitstellen,

während Sie bei der Installation im Silent Mode keine Installationsinformationen angeben müssen.

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 von dem Host zugegriffen werden, auf dem der SnapCenter-Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 SnapCenter Plug-in Loader Service neu.

> Die Installation des Plug-ins-Pakets registriert die Plug-ins auf dem Host und nicht auf dem SnapCenter-Server. Sie sollten die Plug-ins auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Wählen Sie beim Hinzufügen des Hosts als Anmeldeinformationen „Keine“ aus. Nach dem Hinzufügen des Hosts werden die installierten Plug-ins automatisch erkannt.

Installieren Sie Plug-ins Package für AIX im Silent-Modus

Sie können das SnapCenter-Plug-ins-Paket für AIX im Silent-Modus mithilfe der Befehlszeilenschnittstelle (CLI) installieren.

Was Sie brauchen

- Sie sollten die Voraussetzungen für die Installation des Plug-ins-Pakets überprüfen.
- Sie sollten sicherstellen, dass die UMGEBUNGSVARIABLE DISPLAY nicht eingestellt ist.

  Wenn die UMGEBUNGSVARIABLE DISPLAY eingestellt ist, sollten Sie die Anzeige Unset ausführen und anschließend 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 von dem Host zugegriffen werden, auf dem der SnapCenter-Server installiert ist.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 SnapCenter Plug-in Loader Service neu.

> Die Installation des Plug-ins-Pakets registriert die Plug-ins auf dem Host und nicht auf dem SnapCenter-Server. Sie sollten die Plug-ins auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Wählen Sie beim Hinzufügen des Hosts als Anmeldeinformationen „Keine“ aus. Nach dem Hinzufügen des Hosts werden die installierten Plug-ins automatisch erkannt.

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

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 SnapCenter Plug-ins-Paket für AIX installieren.

Über diese Aufgabe

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

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

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

Parametername	Beschreibung
PROTOKOLL_LEVEL	Zeigt die unterstützten Protokollebenen an. Mögliche Werte sind TRACE, DEBUG, INFO, WARN, FEHLER, Und TÖDLICH.
SPL_PROTOKOLL	Zeigt das von SnapCenter Plug-in Loader unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SNAPCENTER_SERVER_PROTOCOL	Zeigt das von SnapCenter-Server unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.

Parametername	Beschreibung
SKIP_JAVAHOME_UPDATE	Standardmäßig erkennt der SPL-Dienst den java-Pfad und aktualisiert DEN JAVA_HOME-Parameter. Daher ist der Standardwert AUF FALSE gesetzt. Sie können auf „TRUE“ setzen, wenn Sie das Standardverhalten deaktivieren und den java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Kennwort der Schlüsselspeicherdatei an. Sie können diesen Wert nur ändern, wenn Sie das Passwort ändern oder eine neue Schlüsselspeicherdatei erstellen.
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Plug-in-Loader ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt. Nach der Installation der Plug-ins sollten Sie den Wert nicht ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter-Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Schlüsselspeicherdatei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.
„LOGS_MAX_COUNT“	Zeigt die Anzahl der SnapCenter-Plug-in-Loader-Protokolldateien an, die im Ordner */Custom_location/snapcenter/spl/logs* aufbewahrt werden. Der Standardwert ist 5000. Wenn der Zähler größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Prüfung auf die Anzahl der Dateien erfolgt automatisch alle 24 Stunden ab dem Start des SnapCenter Plug-in Loader-Dienstes. Wenn Sie die Datei spl.properties manuell löschen, wird die Anzahl der zu behaltenden Dateien auf 9999 festgelegt.

Parametername	Beschreibung
JAVA_HOME	Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird. Dieser Pfad wird während der Installation und im Rahmen des Startens von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Log-Datei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei gezippt und die Protokolle werden in die neue Datei dieses Jobs geschrieben.
BEIBEHALTEN_LOGS_OF_LAST_DAYS	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
ENABLE_CERTIFICATE_VALIDATION	Zeigt true an, wenn die Zertifikatvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder aktivieren oder deaktivieren, indem Sie den spl.properties bearbeiten oder den SnapCenter GUI oder Cmdlet verwenden.

Wenn einer dieser Parameter dem Standardwert nicht zugewiesen ist oder Sie den Wert zuweisen oder ändern möchten, können Sie die Datei spl.properties ändern. Sie können auch die Datei spl.properties überprüfen und die Datei bearbeiten, um Probleme zu beheben, die mit den Werten, die den Parametern zugeordnet sind, zusammenhängen. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter-Plug-in-Loader-Dienst neu starten.

Schritte

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

Sie können die Option -Force mit dem Befehl STOP verwenden, um den SnapCenter Plug-in Loader Dienst nachdrücklich zu stoppen. Vor diesem Verfahren sollten Sie jedoch Vorsicht walten lassen, da auch die bestehenden Vorgänge beendet werden.

- Starten Sie den SnapCenter-Plug-in-Loader-Dienst neu:
  - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
  - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Suchen Sie den Status des SnapCenter-Plug-in-Loader-Dienstes:
  - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
  - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Finden Sie die Änderung im SnapCenter-Plug-in-Loader-Dienst:
  - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

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

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

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

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

Schritte

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

   Dieser Wert entspricht dem Schlüssel 'SPL_KEYSTORE_PASS'.

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

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

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

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

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

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

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

Schritte

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

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

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

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

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

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

Schritte

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

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen
Schlüssel hinzu.
```

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

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

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

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

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

Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.

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

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

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

Schritte

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

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Import der Daten von SnapManager für Oracle und SnapManager für SAP zu 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 Importwerkzeug über die Befehlszeilenschnittstelle (Linux Host CLI) ausführen.

Das Importprogramm erstellt Richtlinien und Ressourcengruppen in SnapCenter. Die in SnapCenter erstellten Richtlinien und Ressourcengruppen entsprechen den Profilen und Vorgängen, die mithilfe dieser Profile in SnapManager für Oracle und SnapManager für SAP durchgeführt wurden. Das Importtool von SnapCenter arbeitet mit den Datenbanken SnapManager für Oracle und SnapManager für SAP sowie mit der zu importierenden Datenbank zusammen.

- Ruft alle Profile, Zeitpläne und Vorgänge ab, die mithilfe der Profile durchgeführt werden.
- Erstellt für jeden eindeutigen Vorgang und jeden mit einem Profil verbundenen Zeitplan eine SnapCenter-Backup-Richtlinie.
- Erstellt für jede Zieldatenbank eine Ressourcengruppe.

Sie können das Import-Tool ausführen, indem Sie das sc-Migrationsskript unter */opt/NetApp/snapcenter/spl/bin* ausführen. Wenn Sie das SnapCenter Plug-ins-Paket für Linux auf dem Datenbank-Host installieren, den Sie importieren möchten, wird das sc-Migration-Skript in */opt/NetApp/snapcenter/spl/bin* kopiert.

Der Datenimport wird von der grafischen SnapCenter-Benutzeroberfläche (GUI) nicht unterstützt.

SnapCenter unterstützt Data ONTAP in 7-Mode nicht. Mit dem 7-Mode Transition Tool können Sie Daten und Konfigurationen, die auf einem System mit Data ONTAP 7-Mode gespeichert sind, auf einem ONTAP System migrieren.

Konfigurationen für den Datenimport unterstützt

Bevor Sie Daten von SnapManager 3.4.x für Oracle und SnapManager 3.4.x für SAP zu SnapCenter importieren, sollten Sie die Konfigurationen kennen, die vom SnapCenter Plug-in für Oracle Database unterstützt werden.

Die Konfigurationen, die vom SnapCenter-Plug-in für Oracle-Datenbank unterstützt werden, sind in der aufgeführt "NetApp Interoperabilitäts-Matrix-Tool".

Was wird nach SnapCenter importiert

Sie können mithilfe der Profile Profile Profile Profile, Zeitpläne und Vorgänge importieren.

Von SnapManager für Oracle und SnapManager für SAP	Für SnapCenter
Profile ohne Vorgänge und Zeitpläne	Eine Richtlinie wird mit dem Standardsicherungstyp „Online“ und dem Backup-Umfang als „voll“ erstellt.

Von SnapManager für Oracle und SnapManager für SAP	Für SnapCenter
Profile mit einem oder mehreren Operationen	Mehrere Richtlinien werden auf der Grundlage einer einzigartigen Kombination eines Profils und der Operationen erstellt, die mit diesem Profil durchgeführt werden. Die in SnapCenter erstellten Richtlinien enthalten die Details zum Archivprotokoll und zur Aufbewahrung, die vom Profil und den entsprechenden Vorgängen abgerufen werden.
Profile mit der Konfiguration von Oracle Recovery Manager (RMAN	Richtlinien werden mit der Option **Katalog Backup mit Oracle Recovery Manager** erstellt. Wenn die externe RMAN Katalogisierung in SnapManager verwendet wurde, müssen Sie die RMAN-Katalogeinstellungen in SnapCenter konfigurieren. Sie können entweder die vorhandenen Anmeldedaten auswählen oder neue Anmeldedaten erstellen. Wenn RMAN über die Steuerdatei in SnapManager konfiguriert wurde, müssen Sie RMAN nicht in SnapCenter konfigurieren.
Mit einem Profil angehängte Planung	Eine Richtlinie wird nur für den Zeitplan erstellt.
Datenbank	Für jede importierte Datenbank wird eine Ressourcengruppe erstellt. In einem RAC-Setup (Real Application Clusters) wird der Knoten, auf dem Sie das Importwerkzeug ausführen, nach dem Import der bevorzugte Knoten und die Ressourcengruppe für diesen Knoten erstellt.

Wenn ein Profil importiert wird, wird zusammen mit der Backup-Richtlinie eine Verifizierungsrichtlinie erstellt.

Wenn SnapManager für Oracle und SnapManager für SAP Profile, Zeitpläne und Vorgänge, die mit den Profilen ausgeführt werden, in SnapCenter importiert werden, werden auch die verschiedenen Parameterwerte importiert.

Parameter und Werte von SnapManager für Oracle und SnapManager für SAP	SnapCenter-Parameter und -Werte	Hinweise
Umfang Des Backups • Voll • Daten • Protokoll	Umfang Des Backups • Voll • Daten • Protokoll	
Backup-Modus • Automatisch • Online • Offline	Backup-Typ • Online • Offline Herunterfahren	Wenn der Backup-Modus automatisch ist, überprüft das Importwerkzeug den Datenbankstatus bei Durchführung des Vorgangs und setzt den Backup-Typ entsprechend entweder als Online- oder Offline-Herunterfahren.
Aufbewahrung • Tage • Zählt	Aufbewahrung • Tage • Zählt	SnapManager für Oracle und SnapManager für SAP benötigt zur Festlegung der Datenhaltung sowohl Tage als auch Zählung. In SnapCenter gibt es entweder Days *ODER* Counts. Die Aufbewahrung wird also in Bezug auf Tage festgelegt, an denen in SnapManager für Oracle und SnapManager für SAP die Präferenz für Tage erhalten wird.
Beschneidung für Schichtpläne • Alle • Systemänderungsnummer (SCN) • Datum • Protokolle, die vor den angegebenen Stunden, Tagen, Wochen und Monaten erstellt wurden	Beschneidung für Schichtpläne • Alle • Protokolle, die vor den angegebenen Stunden und Tagen erstellt wurden	SnapCenter unterstützt keine Hochgau auf Basis von SCN, Datum, Wochen und Monaten.

Parameter und Werte von SnapManager für Oracle und SnapManager für SAP	SnapCenter-Parameter und -Werte	Hinweise
Benachrichtigung • E-Mails werden nur für erfolgreiche Vorgänge gesendet • E-Mails werden nur für fehlgeschlagene Vorgänge gesendet • Sowohl für erfolgreiche als auch für fehlgeschlagene Vorgänge gesendete E-Mails	Benachrichtigung • Immer • Bei Ausfall • Warnung • Fehler	Die E-Mail-Benachrichtigungen werden importiert. Sie müssen den SMTP-Server jedoch manuell über die SnapCenter-Benutzeroberfläche aktualisieren. Der Betreff der E-Mail bleibt leer, damit Sie sie konfigurieren können.

Was wird nicht in SnapCenter importiert

Das Importwerkzeug importiert nicht alles nach SnapCenter.

Folgendes kann nicht in SnapCenter importiert werden:

- Backup von Metadaten
- Teilweise Backups
- RDM (Raw Device Mapping) und Virtual Storage Console (VSC)-bezogene Backups
- Rollen oder Zugangsdaten, die im Repository von SnapManager für Oracle und SnapManager für SAP verfügbar sind
- Daten zu Verifizierungs-, Restore- und Klonvorgängen
- Beschnitt für den Betrieb
- Replikationsdetails, die im Profil SnapManager für Oracle und SnapManager für SAP angegeben sind

  Nach dem Import müssen Sie die entsprechende Richtlinie, die in SnapCenter erstellt wurde, manuell bearbeiten, um die Replikationsdetails einzuschließen.

- Katalogisierte Backup-Informationen

Vorbereitung für den Import von Daten

Bevor Sie Daten in SnapCenter importieren, müssen Sie bestimmte Aufgaben durchführen, um den Importvorgang erfolgreich ausführen zu können.

Schritte

1. Geben Sie die Datenbank an, die Sie importieren möchten.
2. Fügen Sie mithilfe von SnapCenter den Datenbank-Host hinzu und installieren Sie das SnapCenter Plug-ins Paket für Linux.
3. Richten Sie mithilfe von SnapCenter die Verbindungen zu den Storage Virtual Machines (SVMs) ein, die von den Datenbanken auf dem Host verwendet werden.

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 Importwerkzeug ausführen möchten, muss die Datenbank zugänglich sein, sonst schlägt die Erstellung der Ressourcengruppe fehl.

   Wenn die Datenbank Anmeldeinformationen konfiguriert ist, müssen Sie in SnapCenter eine entsprechende Berechtigung erstellen, die Anmeldeinformationen der Datenbank zuweisen und dann die Ermittlung der Datenbank erneut ausführen. Wenn sich die Datenbank auf Automatic Storage Management (ASM) befindet, müssen Sie Anmeldedaten für die ASM-Instanz erstellen und die Anmeldeinformationen der Datenbank zuweisen.
6. Stellen Sie sicher, dass der Benutzer, der das Importwerkzeug ausführt, über ausreichende Berechtigungen verfügt, um SnapManager für Oracle oder SnapManager für SAP CLI-Befehle (z. B. den Befehl zum Unterbrechen von Zeitplänen) von SnapManager für Oracle oder SnapManager für SAP-Host auszuführen.
7. Führen Sie die folgenden Befehle auf dem SnapManager für Oracle oder SnapManager für SAP Host aus, um die Zeitpläne zu unterbrechen:
   a. Wenn Sie die Zeitpläne auf dem SnapManager für Oracle Host unterbrechen möchten, führen Sie folgende Schritte 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 folgende Schritte 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 für jedes Profil auf dem Host den Befehl smsap Credential Set ausführen.
8. Stellen Sie sicher, dass der vollständig qualifizierte Domänenname (FQDN) des Datenbankhosts angezeigt wird, wenn Sie den Hostnamen -f ausführen.

Wenn FQDN nicht angezeigt wird, müssen Sie /etc/Hosts ändern, um den FQDN des Hosts anzugeben.

Daten importieren

Sie können Daten importieren, indem Sie das Importwerkzeug vom Datenbank-Host ausführen.

Über diese Aufgabe

Die nach dem Importieren erstellten SnapCenter Backup-Richtlinien haben unterschiedliche Benennungsformate:

- Richtlinien, die für die Profile ohne Operationen und Zeitpläne erstellt wurden, haben das SM_PROFILNAME_ONLINE_FULL_DEFAULT_MIGRIERTE Format.

  Wenn mit einem Profil kein Vorgang durchgeführt wird, wird die entsprechende Richtlinie mit dem Standard-Backup-Typ als online und im Backup-Umfang vollständig erstellt.

- Richtlinien, die für die Profile mit einem oder mehreren Operationen erstellt wurden, haben das SM_PROFILNAME_BACKUPMODE_BACKUPSCOPE_MIGRIERTE Format.
- Richtlinien, die für die an die Profile angeschlossenen Zeitpläne erstellt wurden, weisen das SM_PROFILNAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRIERTE Format auf.

Schritte

1. Melden Sie sich beim Datenbank-Host an, den Sie importieren möchten.
2. Führen Sie das Import-Tool aus, indem Sie das sc-Migrationsskript unter */opt/NetApp/snapcenter/spl/bin* ausführen.
3. Geben Sie den Benutzernamen und das Kennwort des SnapCenter-Servers ein.

   Nach dem Validieren der Zugangsdaten wird eine Verbindung mit SnapCenter hergestellt.

4. Geben Sie die Datenbankdetails zu SnapManager für Oracle oder SnapManager für SAP ein.

   In der Repository-Datenbank werden die auf dem Host verfügbaren Datenbanken aufgelistet.

5. Geben Sie die Details der Zieldatenbank ein.

   Wenn Sie alle Datenbanken auf dem Host importieren möchten, geben Sie alle ein.

6. Wenn Sie ein Systemprotokoll generieren oder ASUP-Nachrichten für fehlgeschlagene Vorgänge senden möchten, müssen Sie diese entweder aktivieren, indem Sie den Befehl *Add-SmStorageConnection* oder *set-SmStorageConnection* ausführen.

> Wenn Sie einen Importvorgang abbrechen möchten, entweder während des Imports oder nach dem Import, müssen Sie die SnapCenter-Richtlinien, Anmeldedaten und Ressourcengruppen, die im Rahmen des Importvorgangs erstellt wurden, manuell löschen.

Ergebnisse

Die SnapCenter Backup-Richtlinien werden für Profile, Zeitpläne und Vorgänge erstellt, die mithilfe der Profile durchgeführt werden. Ressourcengruppen werden auch für jede Zieldatenbank erstellt.

Nach dem erfolgreichen Import der Daten werden die mit der importierten Datenbank verknüpften Zeitpläne in

SnapManager für Oracle und SnapManager für SAP ausgesetzt.

> Nach dem Importieren müssen Sie die importierte Datenbank oder das Dateisystem mit SnapCenter verwalten.

Die Protokolle für jede Ausführung des Importwerkzeugs werden im Verzeichnis */var/opt/snapcenter/spl/logs* mit dem Namen spl_Migration_timestamp.log gespeichert. In diesem Protokoll können Sie Importfehler überprüfen und beheben.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

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

Konfigurieren Sie die CRL-Datei

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

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

Bereiten Sie sich auf den Schutz von Oracle Datenbanken vor

Bevor Sie Datensicherungsvorgänge wie Backup-, Klon- oder Restore-Vorgänge durchführen, müssen Sie Ihre Strategie definieren und die Umgebung festlegen. Sie können den SnapCenter Server auch zur Verwendung von SnapMirror und SnapVault Technologie einrichten.

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

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

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

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

- Create credentials with Authentication Mode as Linux or AIX for the install user. "Weitere Informationen ."
- Fügen Sie Hosts hinzu, installieren Sie die Plug-ins und ermitteln Sie die Ressourcen.
- Wenn Sie SnapCenter Server zum Schutz von Oracle Datenbanken nutzen, die sich auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.
- Installieren Sie Java auf Ihrem Linux oder AIX Host.

  Weitere Informationen finden Sie unter "Anforderungen an Linux-Hosts" oder "AIX-Host-Anforderungen" .
- Sie sollten den Zeitwert der Anwendungs-Firewall auf 3 Stunden oder mehr einstellen.
- Wenn Sie Oracle Datenbanken in NFS-Umgebungen haben, müssen Sie mindestens eine NFS Daten-LIF für primären oder sekundären Storage konfiguriert haben, um Mount-, Klon-, Verifizierungs- und Restore-Vorgänge durchzuführen.
- Wenn Sie mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration haben, können Sie Folgendes mithilfe der SnapCenter-CLI auf dem Datenbank-Host durchführen:
  - Standardmäßig werden alle IP-Adressen des Datenbank-Hosts der Richtlinie für den NFS-Storage-Export 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 in einer SVM mehrere Datenpfade (LIFs) vorhanden sind, wählt SnapCenter den entsprechenden Datenpfad (LIF) zur Mounten des geklonten NFS-Volumes. Wenn Sie jedoch einen bestimmten Datenpfad (LIF) angeben möchten, müssen Sie die CLI Set-SvmPreferredDataPath ausführen. Das Command Reference Guide enthält weitere Informationen.
- Wenn Sie Oracle-Datenbanken in SAN-Umgebungen nutzen, stellen Sie sicher, dass die SAN-Umgebung gemäß der in den folgenden Leitfäden genannten Empfehlung konfiguriert ist:
  - "Empfohlene Host-Einstellungen für Linux Unified Host Utilities"
  - "Host-Einstellungen, die von AIX Host Utilities betroffen sind"
- Wenn Sie Oracle-Datenbanken auf LVM in Oracle Linux- oder RHEL-Betriebssystemen haben, installieren Sie die neueste Version von Logical Volume Management (LVM).
- Wenn Sie SnapManager für Oracle verwenden und zu SnapCenter Plug-in für Oracle Database migrieren möchten, können Sie die Profile mithilfe des scli-Befehls sc-migrate zu Richtlinien und Ressourcengruppen von SnapCenter migrieren.
- Konfigurieren Sie SnapMirror und SnapVault auf ONTAP, falls Sie eine Backup-Replizierung möchten

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für SnapCenter 4.3.x-Anwender enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Filesysteme mithilfe des Linux-basierten SnapCenter Plug-ins für VMware vSphere Virtual Appliance (Open Virtual Appliance Format).

Weitere Informationen

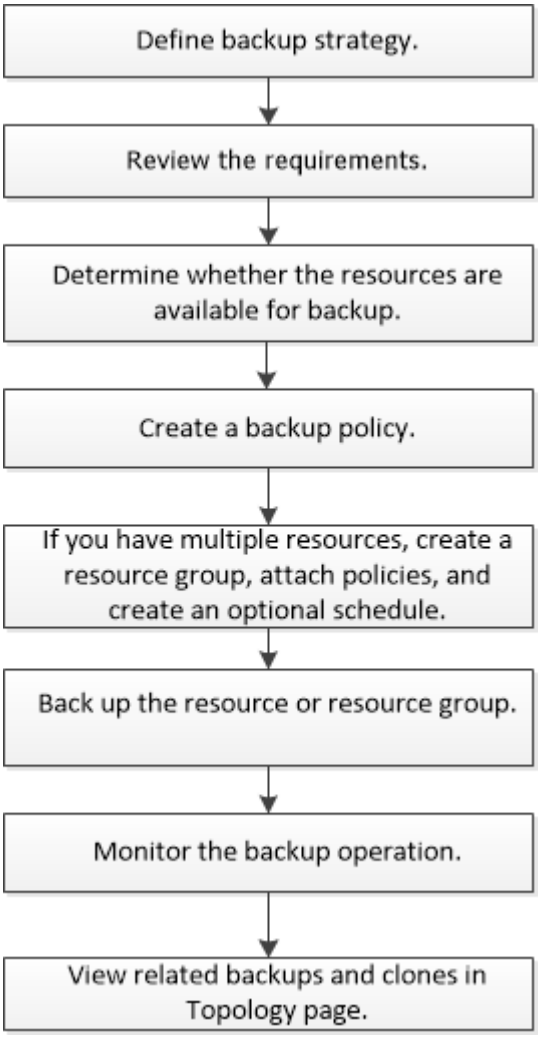
- "Interoperabilitäts-Matrix-Tool"
- "Dokumentation zum SnapCenter Plug-in für VMware vSphere"
- "Die Datensicherung schlägt in einer Umgebung ohne Multipath in RHEL 7 und höher fehl"

Backup von Oracle Datenbanken

Überblick über den Sicherungsvorgang

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Prozess umfasst die Planung, die Ermittlung der Backup-Ressourcen, die Erstellung von Backup-Richtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Backups und die Überwachung von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Während der Erstellung eines Backups für Oracle-Datenbanken wird auf dem Oracle-Datenbank-Host im Verzeichnis */var/opt/snapcenter/sco/lock* eine operative Sperrdatei (*.sm_Lock_dbsid*) erstellt, um zu vermeiden, dass mehrere Operationen auf der Datenbank ausgeführt werden. Nach dem Sichern der Datenbank wird die operative Sperrdatei automatisch entfernt.

Wenn jedoch das vorherige Backup mit einer Warnung abgeschlossen wurde, wird die betriebliche Sperrdatei möglicherweise nicht gelöscht und der nächste Backup-Vorgang in die Warteschleife gelangt. Es kann schließlich abgebrochen werden, wenn die **.SM_Lock_dbsid**-Datei 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 Sie die Betriebssperre:`rm -rf .sm_lock_dbsid.`

Konfigurationsinformationen sichern

Unterstützte Oracle Database Konfigurationen für Backups

SnapCenter unterstützt das Backup verschiedener Oracle Database Konfigurationen.

- Oracle Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container-Datenbank (CDB)
- Oracle Data Guard Standby

  Sie können nur Offline-Mount-Backups von Data Guard Standby-Datenbanken erstellen. Offline-Shutdown-Backup, Backup nur für Archivprotokolle und vollständiges Backup werden nicht unterstützt.

- Oracle Active Data Guard Standby

  Sie können nur Online-Backups von Active Data Guard Standby-Datenbanken erstellen. Backup nur für Archivprotokolle und vollständige Backups werden nicht unterstützt.

  Vor dem Erstellen eines Backups von Data Guard Standby oder der Active Data Guard Standby Datenbank wird der Managed Recovery-Prozess (MRP) angehalten und nach dem Erstellen des Backups wird MRP gestartet.

- Automatisches Storage-Management (ASM)
  - ASM Standalone und ASM RAC auf Virtual Machine Disk (VMDK)

    Unter allen für Oracle-Datenbanken unterstützten Wiederherstellungsmethoden können Sie nur eine Verbindung-und-Kopie-Wiederherstellung von ASM RAC-Datenbanken auf VMDK durchführen.

  - ASM Standalone und ASM RAC on Raw Device Mapping (RDM) + Sie können Backup-, Wiederherstellungs- und Klonvorgänge auf Oracle-Datenbanken auf ASM mit oder ohne ASMLib durchführen.
  - Oracle ASM Filtertreiber (ASMFD)

    PDB-Migration und PDB-Klonvorgänge werden nicht unterstützt.

  - Oracle Flex ASM

Aktuelle Informationen zu unterstützten Oracle-Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Arten von Backups, die für Oracle-Datenbanken unterstützt werden

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt Online- und Offline-Backups für Oracle Datenbanken.

Online-Backup

Ein Backup, das erstellt wird, wenn sich die Datenbank im Online-Status befindet, wird als Online-Backup bezeichnet. Auch als Hot Backup bezeichnet, ermöglicht ein Online-Backup die Erstellung eines Backups der Datenbank, ohne dass es heruntergefahren werden muss.

Im Rahmen des Online-Backups können Sie eine Sicherung der folgenden Dateien erstellen:

- Nur Datendateien und Kontrolldateien
- Nur Archivprotokolldateien (in diesem Szenario wird die Datenbank nicht in den Backup-Modus versetzt)
- Vollständige Datenbank, die Datendateien, Kontrolldateien und Archivprotokolldateien umfasst

Offline-Backup

Ein Backup, das erstellt wird, wenn sich die Datenbank entweder im gemounteten oder Herunterfahrzustand befindet, wird als Offline-Backup bezeichnet. Ein Offline-Backup wird auch als Cold Backup bezeichnet. Sie können nur Datendateien und Steuerdateien in Offline-Backups einbeziehen. Sie können entweder einen Offline-Mount- oder Offline-Shutdown-Backup erstellen.

- Wenn Sie ein Offline-Mount-Backup erstellen, müssen Sie sicherstellen, dass sich die Datenbank in einem gemounteten Zustand befindet.

  Wenn sich die Datenbank in einem anderen Zustand befindet, schlägt der Backup-Vorgang fehl.

- Beim Erstellen einer Offline-Shutdown-Sicherung kann sich die Datenbank in einem beliebigen Zustand befinden.

  Der Datenbankstatus wird in den erforderlichen Zustand geändert, um ein Backup zu erstellen. Nach dem Erstellen des Backups wird der Datenbankzustand in den ursprünglichen Zustand zurückgesetzt.

Wie SnapCenter Oracle Datenbanken erkennt

Bei den Ressourcen handelt es sich um Oracle-Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Diese Datenbanken können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

In den folgenden Abschnitten wird der Prozess beschrieben, den SnapCenter zur Ermittlung verschiedener Typen und Versionen von Oracle-Datenbanken verwendet.

Für Oracle-Versionen 11*g_ bis 12*c__R1

RAC-Datenbank

Die RAC-Datenbanken werden nur anhand von /etc/oratab`Einträgen ermittelt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Standalone

Die eigenständigen Datenbanken werden nur anhand von /etc/oratab-Einträgen ermittelt.

ASM

Der ASM-Instanzeintrag sollte in der Datei /etc/oratab verfügbar sein.

RAC 1-Knoten

Die RAC One Node-Datenbanken werden nur anhand von /etc/oratab-Einträgen ermittelt. Die Datenbanken sollten entweder im nomount-, Mount- oder Open-Zustand sein. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Der RAC One Node Datenbankstatus wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt und Backups mit der Datenbank verknüpft sind.

Wenn die Datenbank verschoben wird, sollten Sie die folgenden Schritte ausführen:

1. Fügen Sie den umgelagerten Datenbankeintrag manuell in der Datei /etc/oratab auf dem Knoten Failed-over RAC hinzu.
2. Aktualisieren Sie die Ressourcen manuell.
3. Wählen Sie auf der Ressourcen-Seite die RAC One Node-Datenbank aus, und klicken Sie dann auf Datenbankeinstellungen.
4. Konfigurieren Sie die Datenbank so, dass die bevorzugten Cluster-Knoten auf den RAC-Knoten eingestellt werden, der derzeit die Datenbank hostet.
5. Führen Sie die SnapCenter Vorgänge aus.
6. Wenn Sie eine Datenbank von einem Knoten auf einen anderen Knoten verschoben haben und der Eintrag Oratab im früheren Knoten nicht gelöscht wird, löschen Sie den Oratab-Eintrag manuell, um zu vermeiden, dass dieselbe Datenbank zweimal angezeigt wird.

Für Oracle Versionen 12cR2 bis 18c

RAC-Datenbank

Die RAC-Datenbanken werden mit dem Befehl srvctl config ermittelt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Standalone

Die eigenständigen Datenbanken werden anhand der Einträge in der Datei /etc/oratab und der Ausgabe des Befehls srvctl config ermittelt.

ASM

Der ASM-Instanzeintrag muss sich nicht in der Datei /etc/oratab befinden.

RAC 1-Knoten

Die RAC One Node-Datenbanken werden nur mit dem Befehl srvctl config ermittelt. Die Datenbanken sollten entweder im nomount-, Mount- oder Open-Zustand sein. Der RAC One Node Datenbankstatus wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt und Backups mit der Datenbank verknüpft sind.

Wenn die Datenbank verschoben wird, sollten Sie die folgenden Schritte ausführen: . Aktualisieren Sie die Ressourcen manuell. . Wählen Sie auf der Ressourcen-Seite die RAC One Node-Datenbank aus, und klicken Sie dann auf Datenbankeinstellungen. . Konfigurieren Sie die Datenbank so, dass die bevorzugten Cluster-Knoten auf den RAC-Knoten eingestellt werden, der derzeit die Datenbank hostet. . Führen Sie die SnapCenter Vorgänge aus.

Wenn in der Datei /etc/oratab Oracle 12*c*R2 und 18*c*-Datenbankeinträge vorhanden sind und dieselbe Datenbank beim Befehl srvctl config registriert ist, beseitigt SnapCenter die doppelten Datenbankeinträge. Wenn veraltete Datenbankeinträge vorhanden sind, wird die Datenbank erkannt, die Datenbank ist jedoch nicht erreichbar und der Status ist offline.

Bevorzugte Knoten im RAC-Setup

In Oracle Real Application Clusters (RAC)-Setup können Sie die bevorzugten Knoten angeben, die SnapCenter für die Durchführung des Backup-Vorgangs verwendet. Wenn Sie den bevorzugten Node nicht angeben, weist SnapCenter automatisch einen Node als bevorzugten Node zu und auf diesem Node wird das Backup erstellt.

Die bevorzugten Knoten können einer oder alle Cluster-Knoten sein, wo 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 node1, cdbrac2 auf node2 und cdbrac3 auf node3.

Die Instanzen node1 und node2 werden als bevorzugte Nodes konfiguriert, wobei node2 die erste Präferenz und node1 als zweite Präferenz. Wenn Sie einen Sicherungsvorgang ausführen, wird in node2 der erste Vorgang versucht, da er der erste bevorzugte Node ist.

Wenn node2 nicht in dem Status zum Sichern ist, was aus mehreren Gründen, wie z. B. dem Plug-in-Agent, auf dem Host nicht ausgeführt werden kann, ist die Datenbankinstanz auf dem Host nicht im erforderlichen Zustand für den angegebenen Backup-Typ, Oder die Datenbankinstanz auf node2 in einer FlexASM-Konfiguration wird nicht von der lokalen ASM-Instanz bereitgestellt; dann wird der Vorgang auf node1 versucht.

Das node3 wird nicht für das Backup verwendet, da es sich nicht auf der Liste der bevorzugten Nodes befindet.

Flex ASM-Einrichtung

In einem Flex ASM-Setup werden Leaf-Knoten nicht als bevorzugte Knoten aufgeführt, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist. Wenn sich Änderungen an den Flex ASM-Cluster-Knotenrollen ergeben, sollten Sie manuell ermitteln, damit die bevorzugten Nodes aktualisiert werden.

Erforderlicher Datenbankstatus

Die RAC-Datenbankinstanzen auf den bevorzugten Nodes müssen den erforderlichen Status aufweisen, damit das Backup erfolgreich abgeschlossen werden kann:

- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im offenen Zustand befinden, um ein Online-Backup 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 ein Offline-Mount-Backup zu erstellen.
- Instanzen von RAC Datenbanken können in jedem Zustand sein. Sie müssen jedoch die bevorzugten Nodes angeben, um ein Offline-Herunterfahren-Backup zu erstellen.

So katalogisieren Sie Backups mit Oracle Recovery Manager

Sie können die Backups von Oracle-Datenbanken mit Oracle Recovery Manager (RMAN) katalogisieren, um die Backup-Informationen im Oracle RMAN-Repository zu speichern.

Die katalogisierten Backups können später für Wiederherstellungen auf Blockebene oder für zeitpunktgenaue Recovery-Vorgänge in Tablespaces verwendet werden. Wenn Sie diese katalogisierten Backups nicht benötigen, können Sie die Kataloginformationen entfernen.

Die Datenbank muss im gemounteten oder höheren Zustand für die Katalogisierung enthalten sein. Sie können Katalogisierung von Daten-Backups, Archivierungs-Log-Backups und vollständigen Backups durchführen. Wenn die Katalogisierung für ein Backup einer Ressourcengruppe mit mehreren Datenbanken aktiviert ist, wird für jede Datenbank eine Katalogisierung durchgeführt. Bei Oracle RAC-Datenbanken wird die Katalogisierung auf dem bevorzugten Knoten durchgeführt, auf dem die Datenbank mindestens gemounted ist.

Wenn Sie Backups 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 Katalogisierung fehl, anstatt sich in die Warteschlange zu stellen.

Externe Katalogdatenbank

Standardmäßig wird die Kontrolldatei der Zieldatenbank zur Katalogisierung verwendet. Wenn Sie eine externe Katalogdatenbank hinzufügen möchten, können Sie diese konfigurieren, indem Sie die Anmeldeinformationen und den TNS-Namen (Transparent Network Substrat) des externen Katalogs mithilfe des Datenbankeinstellungs-Assistenten von der grafischen Benutzeroberfläche von SnapCenter (GUI) 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 Katalogisierung-Option aktiviert haben und gleichzeitig eine Oracle-Backup-Richtlinie über die SnapCenter-GUI erstellen, werden die Backups über Oracle RMAN als Teil des Backup-Vorgangs katalogisiert. Sie können auch eine verzögerte Katalogisierung von Backups durchführen, indem Sie den Befehl ausführen `Catalog-SmBackupWithOracleRMAN` .

Nach der Katalogisierung der Backups können Sie den Befehl ausführen `Get-SmBackupDetails` , um die katalogisierten Backup-Informationen wie das Tag für katalogisierte Datendateien, den Katalogpfad der Steuerdatei und die katalogisierten Archivprotokollspeicherorte abzurufen.

Benennungsformat

Wenn der Name der ASM-Festplattengruppe größer oder gleich 16 Zeichen ist, ab SnapCenter 3.0, lautet das für die Datensicherung verwendete Namensformat SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. Wenn der Name der Laufwerksgruppe jedoch weniger als 16 Zeichen beträgt, ist das für das Backup verwendete Namensformat DISKGROUPNAME_DBSID_BACKUPID, das gleiche Format wie in SnapCenter 2.0.

Die HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Stellen), die für jede ASM-Laufwerksgruppe eindeutig ist.

Crosscheck-Operationen

Sie können crosschecks durchführen, um veraltete RMAN Repository-Informationen über Backups zu aktualisieren, deren Repository-Datensätze nicht ihrem physischen Status entsprechen. Wenn ein Benutzer

zum Beispiel archivierte Protokolle mit einem Betriebssystembefehl von der Festplatte entfernt, zeigt die Steuerdatei immer noch an, dass sich die Protokolle auf der Festplatte befinden, wenn sie sich tatsächlich nicht befinden.

Mit der crosscheck-Operation können Sie die Steuerdatei mit den Informationen aktualisieren. Sie können crosscheck aktivieren, indem Sie den Befehl set-SmConfigSettings ausführen und den Wert TRUE dem PARAMETER ENABLE_CROSSCHECK zuweisen. Der Standardwert ist FALSE.

```
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 mithilfe der SnapCenter-GUI entfernen. Die Informationen eines katalogisierten Backups werden jedoch beim Löschen des Backups oder beim Löschen der mit diesem katalogisierten Backup verknüpften Aufbewahrungs- und Ressourcengruppe entfernt.

> Wenn Sie eine Löschung des SnapCenter-Hosts erzwingen, werden die Informationen der mit diesem Host verbundenen katalogisierten Backups nicht entfernt. Sie müssen die Informationen aller katalogisierten Backups für diesen Host entfernen, bevor Sie die Löschung des Hosts erzwingen.

Wenn die Katalogisierung und Entkatalogisieren fehlschlägt, weil die Betriebsdauer den für DEN PARAMETER ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT angegebenen Zeitwert 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 SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

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

Vordefinierte Umgebungsvariablen für Backup-spezifische Prescript und Postscript

Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie während der Erstellung von Backup-Richtlinien das Prescript und das Postscript ausführen. Diese Funktion wird mit Ausnahme von VMDK für alle Oracle-Konfigurationen unterstützt.

SnapCenter definiert die Werte der Parameter, auf die in der Umgebung, in der die Shell-Skripte ausgeführt werden, direkt zugegriffen werden kann. Bei der Ausführung der Skripte müssen Sie die Werte dieser Parameter nicht manuell angeben.

Unterstützte vordefinierte Umgebungsvariablen für das Erstellen von Backup-Richtlinien

- **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 Datenbanknamen, die per Pipe getrennt sind.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: NFSB32 natürlich NFSB31

- **SC_HOST** gibt den Hostnamen der Datenbank an.

  Bei RAC ist der Hostname der Name des Hosts, auf dem das Backup durchgeführt wird.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** gibt den Betriebssystembesitzer der Datenbank an.

  Die Daten werden als <db1>@<osser1><db2>@<osser2> formatiert.

  Beispiel: NFSB31@oracle NFSB32@oracle

- **SC_OS_GROUP** gibt die Betriebssystemgruppe der Datenbank an.

  Die Daten werden als <db1>@<osgroup1><db2>@<osgroerp2> formatiert.

  Beispiel: NFSB31@Installation von NFSB32@oinstall

- **SC_BACKUP_TYPE**" gibt den Sicherungstyp an (online voll, online Daten, Online log, offline Shutdown, offline Mount)

  Beispiele:

  - Für vollständige Backups: ONLINEFULL
  - Backup nur Daten: OnLINEDATA
  - Für nur-Protokoll-Sicherung: ONLINELOG

- **SC_BACKUP_NAME** gibt den Namen des Backups an.

  Dieser Parameter wird für Anwendungs-Volumes 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 Backup-ID an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

BEISPIEL: DATEN@203 LOG@@205 V/207

- **SC_ORACLE_HOME** gibt den Pfad des Oracle Home-Verzeichnisses an.

  Beispiel: NFSB32@/ora01/App/oracle/Produkt/18.1.0/db_1 natürlich 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: Stündliche DATEN@TAGE:3 natürlich LOG@ANZAHL:4
  - Nur für On-Demand-Datensicherung: OnDemand Daten@COUNT:2
  - Nur für On-Demand-Log-Backup: OnDemand-LOG@COUNT:2
- **SC_RESOURCE_GROUP_NAME** gibt den Namen der Ressourcengruppe an.

  Beispiel: RG1

- **SC_BACKUP_POLICY_NAME** gibt den Namen der Backup Policy an.

  Beispiel: Backup_Policy

- **SC_AV_NAME** gibt die Namen der Anwendungsvolumes an.

  Beispiel: AV1 natürlich AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** gibt die Speicherzuordnung von SVM zu Volume für das Verzeichnis der Datendateien an. Er wird der Name des übergeordneten Volume für luns und qtrees sein.

  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 zu Volume für das Log-Dateiverzeichnis an. Er wird der Name des übergeordneten Volume für luns und qtrees sein.

  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 Volumes 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 02.28.26.3973-21-2021_1_1

- Für mehrere Datenbankinstanzen: NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_CDB_2021_07 02.28.26.3973 2021 21_SB1-17002_SB002_SB71_21_SB71BG_07 02.28.26.3973 2021_21_SB002_SB71B2B2BG_07 02.28.26.3973_SB002_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB002_SB1.01_SB002_SB71.01_SB71.01_SB1.01_SB002_SB002_SB1.01_SB1.01_

- **SC_PRIMARY_SNAPSHOT_NAMES** gibt die Namen der primären Snapshots an, die während des Backups 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 Snapshots der Konsistenzgruppe, 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 Details des Mount-Punkts an, die Teil des Backups sind.

  Zu den Details gehört das Verzeichnis, auf dem Volumes angehängt sind und nicht das unmittelbare übergeordnete Objekt der zu sicherenden Datei. Bei einer ASM-Konfiguration ist dies der Name der Laufwerksgruppe.

  Die Daten werden als <db1>@<mountpoint1,mountpoint2><db2>@<mountpoint1,mountpoint2> formatiert.

  Beispiele:

  - Für 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 Datenbank-Instanz: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfb32_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/b32_nfslog

- **SC_ARCHIVELOGS_LOCATIONS** gibt den Speicherort des Archiv-Log-Verzeichnisses an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Archivprotokolldateien. Wenn die Archivprotokolle an mehreren Orten abgelegt werden, werden alle Speicherorte erfasst. Dazu gehören auch die FRA-Szenarien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_log
  - Für mehrere Datenbanken auf NFS und für die NFSB31 Datenbank-Archiv-Logs, die in zwei verschiedenen Speicherorten platziert sind: NFSB31@/mnt/nsdb31_log1,/mnt/nfsdb31_log2 natürlich NFSB32@/mnt/nfsdb32_log
  - FÜR ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15
- **SC_REDO_LOGS_LOCATIONS** gibt den Speicherort des Verzeichnisses der Wiederherstellungsprotokolle an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Redo-Log-Dateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für 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 Steuerdateien-Verzeichnisses an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Steuerdateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank 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 Verzeichnisses der Datendateien an.

  Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Datendateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

  Beispiele:

  - Für einzelne Datenbank auf NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_Data/NEWDB3/Datendatei
  - 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 Labels an.

  Beispiele: Stündliche, tägliche, wöchentliche, monatliche oder benutzerdefinierte Bezeichnung.

Unterstützte Trennzeichen

- **:** wird zur Trennung von SVM-Name und Volume-Name verwendet

  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 02.28.26.3973-21-2021_1

- **@** wird verwendet, um Daten von ihrem Datenbanknamen zu trennen und den Wert von seinem Schlüssel zu trennen.

  Beispiele:

  - NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21 07 02.28.26.3973 2021 21-2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_SB32_SB00G2_spsprod2417819002_SB1_21_SB1-1271_2021 21 07 02.28.26.3973_SB00DB_SB002_SB71_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB002_SB002_SB00BG_07 02.28.26.3973 2021_SB1.01_SB1.0
  - NFSB31@oracle NFSB32@oracle

- * * Wird verwendet, um die Daten zwischen zwei unterschiedlichen Datenbanken zu trennen und die Daten zwischen zwei verschiedenen Einheiten für SC_BACKUP_ID, SC_BACKUP_RETENTION und SC_BACKUP_NAME Parameter zu trennen.

  Beispiele:

  - DATEN@203 PROTOKOLL@205
  - STÜNDLICHE 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

- **/** dient zur Trennung des Volume-Namens von seinem Snapshot für SC_PRIMARY_SNAPSHOT_NAMES und SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG-Parameter.

  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 02.28.26.3973-21-2021_1_1

- **,** wird verwendet, um einen Satz von Variablen für dieselbe DB zu trennen.

  Beispiel: NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21 07 02.28.26.3973 2021 21-2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_CDB_NF32_REDO_2021 21 07 02.28.26.3973_21_SB001.01_SB1-172_SB002_SB1.01_SB002_SB1.02_SB1.02_SB1.01_SB002_SB1.02_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB002_SB002_SB002_SB00

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Backup-Pläne

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen. So könnten beispielsweise regelmäßige Transaktions-Log-Backups ausreichen, um sicherzustellen, dass Sie die Backups haben, die Sie benötigen. Je öfter Sie Ihre Datenbanken sichern, desto weniger Transaktions-Logs benötigt SnapCenter zum Zeitpunkt der Wiederherstellung, was zu schnelleren Restore-Vorgängen führen kann.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder

monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Backups konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Konventionen bei Backup-Namen

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

`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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Anforderungen für das Backup einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank sichern, sollten Sie sicherstellen, dass die Voraussetzungen abgeschlossen sind.

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Sie müssen das Aggregat, das vom Backup-Vorgang verwendet wird, der von der Datenbank verwendeten

Storage Virtual Machine (SVM) zugewiesen haben.

- Sie sollten überprüft haben, ob alle zu der Datenbank gehörenden Daten-Volumes und Archivprotokoll-Volumes geschützt sind, wenn für diese Datenbank ein sekundärer Schutz aktiviert ist.
- Sie sollten überprüfen, dass die Datenbank, die Dateien auf den ASM-Laufwerksgruppen enthält, entweder im Status „`MOUNT`“ oder „`OPEN`“ liegt, um die Backups mit dem Dienstprogramm Oracle DBVERIFY zu überprüfen.
- Sie sollten überprüfen, ob die Länge des Mount-Punkts für das Volumen 240 Zeichen nicht überschreitet.
- Der Wert von RESTTimeout sollte auf 86400000 ms erhöht werden in *C:\Programme\NetApp \SMCore\SMCoreServiceHost.exe.config* Datei auf dem SnapCenter-Server-Host, wenn die zu sichernde Datenbank groß ist (Größe in TB).

  Während Sie die Werte ändern, stellen Sie sicher, dass keine laufenden Jobs vorhanden sind, und starten Sie den SnapCenter SMCore-Dienst nach Erhöhung des Werts neu.

Entdecken Sie die für Backups verfügbaren Oracle-Datenbanken

Ressourcen sind Oracle Datenbanken auf dem Host, die von SnapCenter gemanagt werden. Diese Datenbanken können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

Bevor Sie beginnen

- Sie müssen Aufgaben wie das Installieren des SnapCenter-Servers, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Wenn die Datenbanken auf einer Virtual Machine Disk (VMDK) oder RDM (Raw Device Mapping) befinden, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.

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

- Wenn sich Datenbanken auf einem VMDK-Dateisystem befinden, müssen Sie sich bei vCenter angemeldet und in **VM-Optionen** > **Erweitert** > **Konfiguration bearbeiten** navigiert haben, um den Wert von *Disk.enableUUID* auf true für die VM festzulegen.
- Sie müssen den Prozess überprüft haben, den SnapCenter befolgt, um verschiedene Typen und Versionen von Oracle Datenbanken zu ermitteln.

Schritt 1: SnapCenter daran hindern, nicht-Datenbank-Einträge zu erkennen

Sie können verhindern, dass SnapCenter nicht-Datenbank-Einträge entdeckt, die in der oratab-Datei hinzugefügt wurden.

Schritte

1. Nach der Installation des Plug-ins für Oracle sollte der Root-Benutzer die Datei **sc_oratab.config** unter dem Verzeichnis */var/opt/snapcenter/sco/etc/* erstellen.

   Gewähren Sie dem Oracle Binäreigentümer und der Gruppe die Schreibberechtigung, damit die Datei zukünftig beibehalten werden kann.

2. Der Datenbankadministrator sollte die nicht-Datenbankeinträge in die Datei **sc_oratab.config** hinzufügen.

Es wird empfohlen, dasselbe Format beizubehalten, das für die nicht aus Datenbanken stammenden Einträge in der */etc/oratab*-Datei definiert ist, oder der Benutzer kann einfach die Entity-Zeichenfolge hinzufügen, die nicht aus der Datenbank stammt.

Die Groß-/Kleinschreibung des Strings wird beachtet. 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 Einträge, die nicht aus Datenbanken in der Seite **sc_oratab.config** hinzugefügt wurden, werden auf der Seite Ressourcen nicht aufgeführt.

Es wird immer empfohlen, vor dem Upgrade des SnapCenter-Plug-ins eine Sicherung der sc_oratab.config-Datei zu erstellen.

Schritt 2: Entdecken Sie Ressourcen

Nach der Installation des Plug-ins werden alle Datenbanken auf diesem Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Die Datenbanken sollten sich mindestens im angehängten Zustand oder oben befinden, damit die Datenbanken erfolgreich erkannt werden können. In einer Oracle Real Application Clusters (RAC)-Umgebung sollte sich die RAC-Datenbankinstanz auf dem Host, auf dem die Ermittlung ausgeführt wird, mindestens im gemounteten Zustand oder oben befinden, damit die Datenbankinstanz erfolgreich ermittelt werden kann. Nur die erfolgreich erkannten Datenbanken können den Ressourcengruppen hinzugefügt werden.

Wenn Sie eine Oracle-Datenbank auf dem Host gelöscht haben, ist SnapCenter-Server nicht bekannt und führt die gelöschte Datenbank auf. Sie sollten die Ressourcen manuell aktualisieren, um die Liste der SnapCenter-Ressourcen 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 Sie auf , und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern. Sie können dann auf das Symbol klicken , um das Filterfenster zu schließen.

3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   In einem RAC-Szenario mit einem Knoten 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 Cluster-Name, zugeordnete 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 Storage-System außerhalb von NetApp befindet, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ einen für die Backup-Meldung nicht verfügbaren Status an.

  Sie können keine Datensicherungsvorgänge für die Datenbank ausführen, die sich auf einem Storage-System anderer Anbieter befindet.

- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und nicht geschützt ist, wird auf der Benutzeroberfläche in der Spalte Gesamtstatus eine nicht geschützte Meldung angezeigt.
- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte „Gesamtstatus“ eine für die Datensicherung verfügbare Meldung an.

Wenn Sie eine Oracle-Datenbankauthentifizierung aktiviert haben, wird in der Ansicht Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Sie müssen Datenbankanmeldeinformationen konfigurieren, um die Datenbank schützen oder zur Ressourcengruppe hinzufügen zu können, um Datensicherungsvorgänge durchzuführen.

Erstellung von Backup-Richtlinien für Oracle Datenbanken

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

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben.
- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erkennen von Datenbanken und das Erstellen von Speichersystemverbindungen ausführen.
- Wenn Sie Snapshots auf einen sekundären gespiegelten oder Vault-Storage replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Ziel-Volumes zugewiesen haben.

- Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript zuweisen.
- Prüfen Sie die spezifischen Voraussetzungen und Einschränkungen von SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektgrenzen für die aktive SnapMirror Synchronisierung".

Über diese Aufgabe

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

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

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

  Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Wählen Sie in der Dropdown-Liste * Oracle Database* aus.
4. Klicken Sie Auf **Neu**.
5. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
6. Führen Sie auf der Seite Sicherungstyp die folgenden Schritte durch:
   - Wenn Sie **ein Online-Backup erstellen** möchten, wählen Sie **Online-Backup**.

     Sie müssen angeben, ob Sie alle Datendateien, Kontrolldateien und Archivprotokolldateien, nur Datendateien und Kontrolldateien oder nur Archivprotokolldateien sichern möchten.
   - Wenn Sie **ein Offline-Backup** erstellen möchten, wählen Sie **Offline-Backup** aus, und wählen Sie dann eine der folgenden Optionen aus:
     - Wenn Sie eine Offline-Sicherung erstellen möchten, wenn sich die Datenbank im Bereitstellungszustand befindet, wählen Sie **Mount**.
     - Wenn Sie eine Offline-Shutdown-Sicherung erstellen möchten, indem Sie die Datenbank in den Shutdown-Status ändern, wählen Sie **Shutdown** aus.

       Wenn Sie über steckbare Datenbanken (PDBs), und möchten den Zustand der PDBs vor der Erstellung des Backups speichern, müssen Sie **Save State of PDBs** wählen. Dies ermöglicht Ihnen, die PDBs in den ursprünglichen Zustand zu bringen, nachdem das Backup erstellt wurde.
   - Geben Sie die Zeitplanhäufigkeit an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

Sie können den Zeitplan (Startdatum und Enddatum) für den Backup-Vorgang festlegen, während Sie eine Ressourcengruppe erstellen. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- Wenn Sie das Backup mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Katalog-Backup mit Oracle Recovery Manager (RMAN)** aus.

  Sie können die Katalogisierung für ein Backup auf einmal entweder über die Benutzeroberfläche oder über den SnapCenter-CLI-Befehl Catalog-SmBackupWithOracleRMAN aufgeschobenen.

  Wenn Sie Backups 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 Katalogisierung fehl, anstatt sich in die Warteschlange zu stellen.

- Wenn Sie Archivprotokolle nach Backup beschneiden möchten, wählen Sie **Prune Archivprotokolle nach Backup** aus.

  Das Beschneiden von Archivprotokollen aus dem Archiv-Protokollziel, das in der Datenbank nicht konfiguriert ist, wird übersprungen.

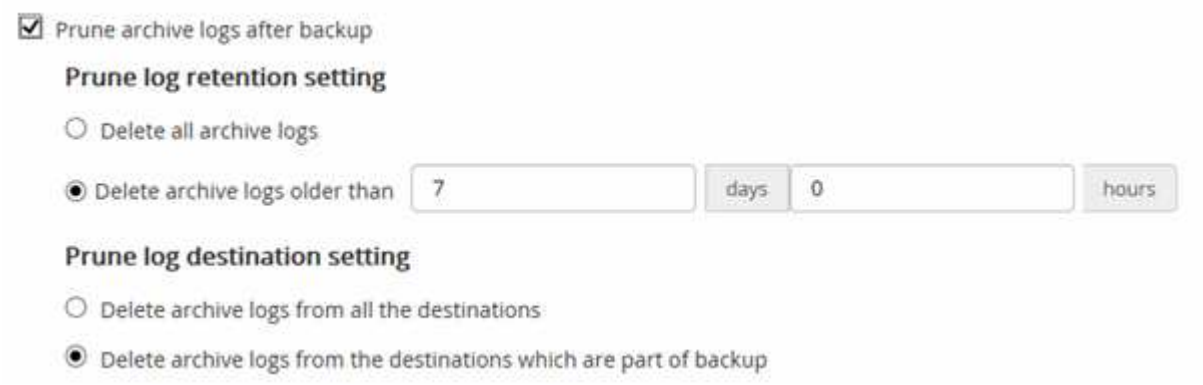
  Wenn Sie Oracle Standard Edition verwenden, können Sie WÄHREND der Sicherung des Archivprotokolls DIE Parameter LOG_ARCHIVE_DEST und LOG_ARCHIVE_DUPLEX_DEST verwenden.

- 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 Archivprotokolle zugreifen können, damit der Löschvorgang erfolgreich ist.

Ihr Ziel ist	Dann…
Löschen Sie alle Archivprotokolle	Wählen Sie **Alle Archivprotokolle löschen**.
Löschen alter Archivprotokolle	Wählen Sie **Archivprotokolle löschen, die älter als** sind, und geben Sie dann das Alter der Archivprotokolle an, die in Tagen und Stunden gelöscht werden sollen.
Löschen Sie Archivprotokolle von allen Zielen	Wählen Sie **Archivprotokolle von allen Zielen löschen**.
Löschen Sie die Archivprotokolle von den Protokollzielen, die Teil des Backups sind	Wählen Sie **Archivprotokolle aus den Zielen löschen, die Teil der Datensicherung sind**.

+



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

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Total Snapshot Copies to keep** aus, und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Snapshot-Kopien behalten für**, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots vor dem Löschen behalten möchten.
Sperrfrist von Snapshots	Wählen Sie die Sperrfrist für Snapshot Kopien aus und wählen Sie Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

Sie können Archiv-Protokoll-Backups nur dann aufbewahren, wenn Sie die Archiv-Log-Dateien als Teil Ihrer Sicherung ausgewählt haben.

8. Geben Sie auf der Seite Replikation die Replikationseinstellungen an:

Für dieses Feld…	**Tun Sie das…**
Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Diese Option sollte für SnapMirror Active Sync aktiviert sein. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden.
Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen. Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert. Weitere Informationen zu SnapLock Vault finden Sie unter "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel" Siehe "Sehen Sie sich Backups und Klone von Oracle Datenbanken auf der Seite Topologie an".

Für dieses Feld…	Tun Sie das…
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

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

   Die Voreinstellungen und Postskripte müssen entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

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

   Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Skript und das Postscript ausführen. "Weitere Informationen ."

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

    a. Wählen Sie den Backup-Zeitplan aus, für den Sie den Verifizierungsvorgang durchführen möchten.

    b. Geben Sie im Abschnitt Skriptbefehle überprüfen den Pfad und die Argumente des Preskript oder Postscript ein, die vor bzw. nach der Verifikation ausgeführt werden sollen.

       Die Voreinstellungen und Postskripte müssen entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

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

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Oracle-Datenbanken

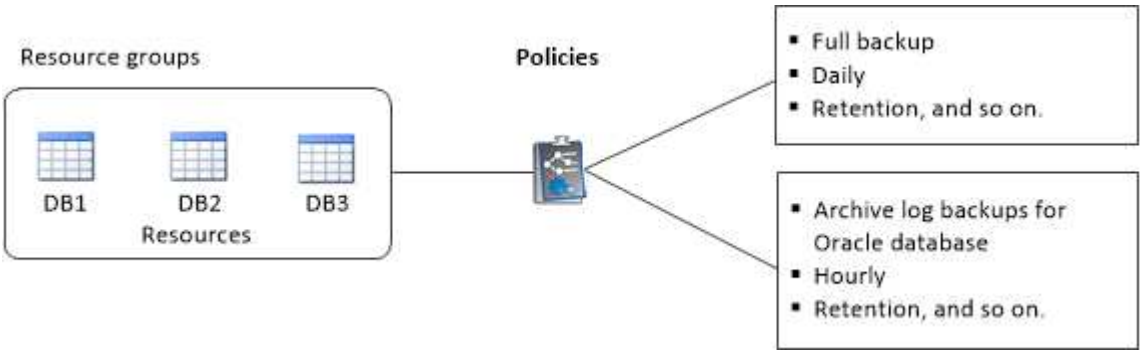
Eine Ressourcengruppe ist ein Container, in dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die einer bestimmten Anwendung zugeordnet sind, gleichzeitig sichern.

Über diese Aufgabe

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

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

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



- Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Das Hinzufügen neuer 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-Status Ressourcen hinzufügen.

Schritte

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

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

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

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

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

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

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

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

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

   Sie können Datenbanken von Linux- und AIX-Hosts in einer einzigen Ressourcengruppe hinzufügen.

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

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

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

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

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

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

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

      Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

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

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

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

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

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

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Oracle-Ressourcen sichern

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

Schritte

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

   Sie können dann klicken , um den Filterbereich zu schließen.
4. Wählen Sie die Datenbank aus, die Sie sichern möchten.

Die Seite Datenbankschutz wird angezeigt.

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

      Zum Beispiel, `customtext_policy_hostname` oder `resource_hostname`. Standardmäßig wird ein Zeitstempel an den Snapshot Namen 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 Dropdown-Liste aus.

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

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

   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf + , um einen Zeitplan für die gewünschte Richtlinie zu konfigurieren.
   c. Konfigurieren Sie im Fenster Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann `OK`.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.
7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Klicken Sie auf **Load Locators**, um die SnapMirror- oder SnapVault-Volumes zu laden, um den sekundären Speicher zu überprüfen.
   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf + , um den Überprüfungsplan für alle Zeitplantypen der Richtlinie zu konfigurieren. + im Dialogfeld Überprüfungszeitpläne hinzufügen *Policy_Name* 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 Dropdown-Liste aus.

      In einem Flex ASM-Setup können Sie auf Leaf-Knoten keine Verifizierungsvorgang durchführen, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist.

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

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

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

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

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

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

   Die Seite der Datenbanktopologie wird angezeigt.

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

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

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

Nachdem Sie fertig sind

- Im AIX-Setup können Sie mit dem `lkdev` Befehl zum Sperren und mit dem `rendev` Befehl die Festplatten umbenennen, auf denen sich die gesicherte Datenbank befand.

  Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mit diesem Backup 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 das Cmdlet ausführen `Set-SmConfigSettings`:

  Nachdem Sie den Wert der Parameter 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`

- Wenn die Datei nicht zugänglich ist und der Mount-Punkt während des Verifizierungsvorgangs nicht verfügbar ist, kann der Vorgang mit dem Fehlercode DBV-00100 der angegebenen Datei fehlschlagen. 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 Dienst SnapCenter Plug-in Loader (SPL) neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

- In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine

Sicherungsbeziehung erkennen.

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java Heap-Größe für das SnapCenter-Plug-in für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

  Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei */opt/netapp/init_scripts/scvservice*. In diesem Skript startet der `do_start method` Befehl den SnapCenter VMware Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Weitere Informationen

- "SnapMirror oder SnapVault-Beziehung kann nach MetroCluster Failover nicht erkannt werden"
- "Oracle RAC One-Knoten-Datenbank wird zur Durchführung von SnapCenter-Operationen übersprungen"
- "Fehler beim Ändern des Status einer Oracle 12c ASM-Datenbank"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen" (Anmeldung erforderlich)

Sichern Sie Oracle Database Resource Groups

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Der Backup-Vorgang wird für alle Ressourcen durchgeführt, die in der Ressourcengruppe definiert sind.

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

Schritte

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

   Klicken Sie auf , um das Filterfenster zu schließen.

4. Wählen Sie auf der Seite Ressourcengruppe die Ressourcengruppe aus, die gesichert werden soll.

   Wenn Sie eine gebündelte Ressourcengruppe mit zwei Datenbanken haben und eine Daten auf nicht-NetApp Speicher hat, wird der Backup-Vorgang abgebrochen, obwohl sich die andere Datenbank auf NetApp Speicher befindet.

5. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie mehrere Richtlinien mit der Ressourcengruppe verknüpft haben, wählen Sie die zu verwendende Sicherungsrichtlinie aus der Dropdown-Liste **Policy** aus.

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

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

Nachdem Sie fertig sind

- Im AIX-Setup können Sie mit dem `lkdev` Befehl zum Sperren und mit dem `rendev` Befehl die Festplatten umbenennen, auf denen sich die gesicherte Datenbank befand.

  Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Wiederherstellungsvorgang, wenn Sie die Wiederherstellung mit diesem Backup 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 das Cmdlet ausführen `Set-SmConfigSettings`:

  Nachdem Sie den Wert der Parameter 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`

- Wenn die Datei nicht zugänglich ist und der Mount-Punkt während des Verifizierungsvorgangs nicht verfügbar ist, kann der Vorgang mit dem Fehlercode DBV-00100 der angegebenen Datei fehlschlagen. 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 Dienst SnapCenter Plug-in Loader (SPL) neu, indem Sie den folgenden Befehl ausführen `/opt/NetApp/snapcenter/spl/bin/spl restart`

Überwachen Sie das Backup von Oracle Datenbanken

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

Überwachen Sie die Backup-Vorgänge für die Oracle Datenbank

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

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.

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

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

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

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

Überwachen Sie Datensicherungsvorgänge im Teilfenster „Vorgang“

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

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

Schritte

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

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

Andere Backup-Vorgänge

Sichern Sie Oracle Datenbanken mit UNIX Befehlen

Der Backup-Workflow umfasst die Planung, die Ermittlung der Backup-Ressourcen, die Erstellung von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Was Sie brauchen

- Sie sollten die Verbindungen zum Speichersystem hinzugefügt und die Anmeldedaten mit den Befehlen *Add-SmStorageConnection* und *Add-SmCredential* erstellt haben.
- Sie sollten die Verbindungssitzung mit dem SnapCenter-Server mit dem Befehl *Open-SmConnection* eingerichtet haben.

Sie können nur eine SnapCenter-Konto-Anmeldesitzung haben und das Token wird im Home-Verzeichnis des Benutzers gespeichert.

Die Verbindungssitzung ist nur 24 Stunden lang gültig. Sie können jedoch ein Token mit der Option TokenNeverExpires erstellen, um ein Token zu 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, die Sicherung und Überprüfung des Backups durchzuführen.

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

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer: *Open-SmConnection*
2. Führen Sie Host-Ressourcen Discovery-Vorgang durch: *Get-SmResources*
3. Konfigurieren Sie die Anmeldeinformationen für Oracle-Datenbanken und bevorzugte Knoten für den Backup-Betrieb einer RAC-Datenbank (Real Application Cluster): *Configure-SmOracleDatabase*
4. Backup-Richtlinie erstellen: *Add-SmPolicy*
5. Abrufen der Informationen zum sekundären Speicherort (SnapVault oder SnapMirror) : *get-SmSecondaryDetails*

   Dieser Befehl ruft Details zur Zuordnung von primärem zu sekundärem Speicher einer bestimmten Ressource ab. Sie können die Zuordnungsdetails verwenden, um die sekundären Verifizierungseinstellungen beim Erstellen einer Backup-Ressourcengruppe zu konfigurieren.
6. Eine Ressourcengruppe zu SnapCenter hinzufügen: *Add-SmResourceGroup*
7. Backup erstellen: *New-SmBackup*

   Sie können den Job mit der Option WaitForCompletion abfragen. Wenn diese Option angegeben ist, fragt der Befehl den Server bis zum Abschluss des Backup-Jobs ab.
8. Abrufen der Protokolle von SnapCenter: *Get-SmLogs*

Backup-Vorgänge von Oracle-Datenbanken abbrechen

Sie können Backup-Vorgänge, die ausgeführt werden, in die Warteschlange gestellt oder nicht ansprechbar sind, abbrechen.

Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Backup-Vorgänge abzubrechen.

Über diese Aufgabe

Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter-Server den Vorgang und entfernt alle

Snapshots aus dem Speicher, wenn das erstellte Backup nicht beim SnapCenter-Server registriert ist. Wenn das Backup bereits beim SnapCenter-Server registriert ist, wird ein Rollback des bereits erstellten Snapshots selbst dann nicht durchgeführt, wenn der Abbruch ausgelöst wurde.

- Sie können nur den Protokoll- oder Vollbackup-Vorgang abbrechen, der in die Warteschlange oder in Betrieb ist.
- Sie können den Vorgang nicht abbrechen, nachdem die Überprüfung gestartet wurde.

  Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Verifizierungsvorgang wird nicht durchgeführt.
- Sie können den Sicherungsvorgang nicht abbrechen, nachdem der Katalogvorgang gestartet wurde.
- Sie können einen Sicherungsvorgang entweder über die Seite Überwachen oder über den Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter GUI können Sie CLI-Befehle verwenden, um Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Vorgang aus und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Initiieren des Backupjobs auf das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Ergebnisse

Der Vorgang wird abgebrochen und die Ressource wird in den ursprünglichen Zustand zurückgesetzt.

Wenn der Vorgang, den Sie abgebrochen haben, im Status Abbrechen oder Ausführen nicht reagiert, sollten Sie Cancel-SmJob -JobID <int> -Force ausführen, um den Backup-Vorgang eindringlich zu beenden.

Sehen Sie sich Backups und Klone von Oracle Datenbanken auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und

sekundären Storage anzuzeigen.

Über diese Aufgabe

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

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

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

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

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

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

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

Schritte

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

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

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

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone sowie die Gesamtanzahl der Backup-Protokolle angezeigt.

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

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

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

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

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

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

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

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um die Wiederherstellung, den Clone, Mount, unmounten, umbenennen, Katalogisieren, Entkatalogisieren und Löschen von Vorgängen

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

   - Wenn Sie eine Protokollsicherung ausgewählt haben, können Sie nur umbenennen, mounten, unmounten, Katalog, Katalog aufheben, Katalog aufheben, Und -Lösch.
   - Wenn Sie das Backup mit dem Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Backups nicht umbenennen.

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

Wenn der für SnapmirrorStatusUpdateWaitTime zugewiesene Wert kleiner ist, werden die Backup-Kopien von Mirror und Vault nicht auf der Topologieseite aufgeführt, auch wenn Daten- und Protokoll-Volumes erfolgreich geschützt sind. Sie sollten den Wert erhöhen, der SnapmirrorStatusUpdateWaitTime mit dem Cmdlet *Set-*

SmConfigSettings PowerShell zugewiesen wurde.

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden.

Alternativ können Sie auch auf oder verweisen "SnapCenter Software Command Reference Guide" "SnapCenter Software Cmdlet Referenzhandbuch".

Binden Sie Datenbank-Backups ein und heben Sie sie ab

Sie können einzelne oder mehrere Daten mounten und Backups protokollieren, wenn Sie auf die Dateien im Backup zugreifen möchten. Sie können das Backup entweder auf demselben Host, auf dem das Backup erstellt wurde, oder auf einem Remote-Host mit denselben Oracle- und Host-Konfigurationen mounten. Wenn Sie die Backups manuell gemountet haben, sollten Sie die Bereitstellung der Backups nach Abschluss des Vorgangs manuell aufheben. Bei jeder beliebigen Instanz kann ein Backup einer Datenbank auf einen beliebigen Host eingebunden werden. Während eines Vorgangs können Sie nur ein einzelnes Backup mounten.

In einem Flex ASM-Setup können Sie den Mount-Vorgang auf Leaf-Knoten nicht ausführen, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist.

Mounten Sie ein Datenbank-Backup

Sie sollten eine Datenbanksicherung manuell mounten, wenn Sie auf die Dateien im Backup zugreifen möchten.

Was Sie brauchen

- Wenn Sie in einer NFS-Umgebung über eine Instanz für Automatic Storage Management (ASM)-Datenbank verfügen und die ASM-Backups mounten möchten, sollten Sie den ASM-Festplattenpfad */var/opt/snapcenter/sco/Backup*/*/*/*/*/_*/* in den im parameter asm_diskstring festgelegten Pfad eingefügt haben.
- Wenn Sie über eine ASM-Datenbankinstanz in einer NFS-Umgebung verfügen und die ASM-Protokollsicherungen im Rahmen eines Wiederherstellungsvorgangs mounten möchten, sollten Sie den ASM-Festplattenpfad */var/opt/snapcenter/scu/Clones/*/** zu dem im parameter asm_diskstring definierten Pfad hinzugefügt haben.
- Im parameter asm_diskstring sollten Sie *AFD:** konfigurieren, wenn Sie ASMFD verwenden oder *ORCL:** konfigurieren, 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-Anmeldedaten und den ASM-Port konfigurieren, wenn er sich von der des Quelldatenbank-Hosts während des Mounten des Backups unterscheidet.
- Wenn Sie ein Mount an einen alternativen Host mounten möchten, müssen Sie überprüfen, dass der alternative Host die folgenden Anforderungen erfüllt:
  - Dieselbe UID und dieselbe GID wie beim ursprünglichen Host

- Dieselbe Oracle Version wie die des ursprünglichen Hosts
- Betriebssystemverteilung und -Version wie beim ursprünglichen Host
- Für NVMe sollte NVMe util installiert werden

- Sie sollten sicherstellen, dass die LUN nicht dem AIX-Host mit iGroup zugeordnet ist, die aus gemischten Protokollen iSCSI und FC besteht. Weitere Informationen finden Sie unter "Der Vorgang schlägt fehl, da der Fehler nicht in der Lage ist, das Gerät für die LUN zu ermitteln".

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus dem 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 Mount Backups den Host aus, auf dem Sie das Backup mounten möchten, aus der Dropdown-Liste **Wählen Sie den Host aus, um die Backup**-Sicherung zu mounten.

   Der Mount-Pfad */var/opt/snapcenter/sco/Backup_Mount/Backup_Name/Database_Name* wird angezeigt.

   Wenn Sie das Backup einer ASM-Datenbank mounten, wird der Mount Path +diskgroupname_SID_Backup angezeigt.

7. Klicken Sie Auf **Mount**.

Nach Ihrer Beendigung

- Sie können den folgenden Befehl ausführen, um die Informationen bezüglich des gemounteten Backups abzurufen:

  ```
  ./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
  ```

- Wenn Sie eine ASM-Datenbank angehängt haben, können Sie den folgenden Befehl ausführen, um die Informationen zu dem gemounteten Backup abzurufen:

  ```
  ./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
  ```

- Führen Sie zum Abrufen der Backup-ID den folgenden Befehl aus:

  ```
  ./sccli Get-Smbackup-BackupNamebackup_name
  ```

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

Heben Sie die Bereitstellung eines Datenbank-Backups auf

Sie können die Bereitstellung einer gemounteten Datenbanksicherung manuell aufheben, wenn Sie nicht mehr auf Dateien im Backup 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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.

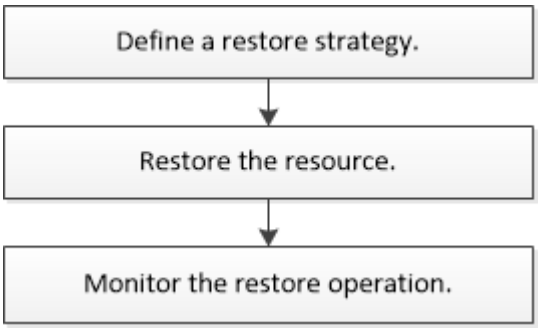
4. Wählen Sie das gemountete Backup aus, und klicken Sie dann auf  .
5. Klicken Sie auf **OK**.

Stellen Sie Oracle Datenbanken wieder her

Wiederherstellung des Workflows

Der Restore-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Definition einer Restore- und Recovery-Strategie für Oracle Datenbanken

Sie müssen eine Strategie definieren, bevor Sie Ihre Datenbank wiederherstellen und wiederherstellen, damit Restore- und Recovery-Vorgänge erfolgreich durchgeführt werden können.

Arten von Backups, die für Wiederherstellungs- und Recovery-Vorgänge unterstützt werden

SnapCenter unterstützt die Wiederherstellung und Wiederherstellung unterschiedlicher Arten von Oracle Datenbank-Backups.

- Online Daten-Backup

- Offline Herunterfahren Datensicherung
- Datensicherung für Offline-Mounten

> Wenn Sie eine Offline-Abschaltung oder Offline-Bereitstellung von Daten-Backups durchführen, lässt SnapCenter die Datenbank in den Offline-Zustand. Sie sollten die Datenbank manuell wiederherstellen und die Protokolle zurücksetzen.

- Vollständiges Backup
- Offline-Mount-Backups von Data Guard Standby-Datenbanken
- Reine Online-Backups von Active Data Guard Standby-Datenbanken

> Sie können keine Wiederherstellung von Active Data Guard Standby-Datenbanken durchführen.

- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer RAC-Konfiguration (Real Application Clusters)
- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer ASM-Konfiguration (Automatic Storage Management)

Arten von Wiederherstellungsmethoden, die für Oracle-Datenbanken unterstützt werden

SnapCenter unterstützt Connect-and-Copy oder in-Place-Restore für Oracle Datenbanken. Während eines Wiederherstellungsvorgangs bestimmt SnapCenter die Wiederherstellungsmethode, die für die Wiederherstellung des Dateisystems ohne Datenverlust geeignet ist.

> SnapCenter bietet keine Unterstützung für Volume-basierte SnapRestore.

Wiederherstellung von Verbindungen und Kopien

Unterscheidet sich das Datenbanklayout von dem Backup, oder gibt es nach dem Backup neue Dateien, so wird die Wiederherstellung der Connect-and-Copy durchgeführt. In der Methode zum Wiederherstellen von Connect-and-Copy werden die folgenden Aufgaben ausgeführt:

Schritte

1. Das Volume wird aus dem Snapshot geklont, und der Filesystem-Stack wird auf dem Host unter Verwendung der geklonten LUNs oder Volumes erstellt.
2. Die Dateien werden von den geklonten Dateisystemen in die ursprünglichen Dateisysteme kopiert.
3. Die geklonten Filesysteme werden dann vom Host abgehängt und die geklonten Volumes werden aus den ONTAP gelöscht.

> Bei einem Flex ASM-Setup (bei dem die Kardinalität kleiner ist als die Anzahl Nodes im RAC-Cluster) oder ASM RAC-Datenbanken auf VMDK oder RDM wird nur die Connect-and-Copy-Wiederherstellungsmethode unterstützt.

Auch wenn Sie die Wiederherstellung vor Ort mit Nachdruck aktiviert haben, führt SnapCenter die Wiederherstellung von Connect und Copy in den folgenden Szenarien durch:

- Wiederherstellung aus einem sekundären Storage-System und bei Data ONTAP vor 8.3

- Wiederherstellen von ASM-Laufwerksgruppen auf Knoten eines Oracle RAC-Setups, auf denen die Datenbankinstanz nicht konfiguriert ist
- Wenn in Oracle RAC-Setup auf einem der Peer-Nodes nicht die ASM-Instanz oder die Cluster-Instanz ausgeführt wird oder wenn der Peer-Node nicht verfügbar ist
- Restore von Kontrolldateien
- Stellen Sie einen Teil der Tabellen aus, die sich in einer ASM-Festplattengruppe befinden, wieder her
- Die Laufwerksgruppe wird zwischen Datendateien, sp-Datei und Kennwortdatei freigegeben
- Der SnapCenter-Plug-in-Loader-Service (SPL) ist nicht auf dem Remote-Knoten in einer RAC-Umgebung installiert oder wird nicht ausgeführt
- Dem Oracle RAC werden neue Knoten hinzugefügt, und der SnapCenter-Server kennt die neu hinzugefügten Knoten nicht

In-Place-Wiederherstellung

Wenn das Datenbank-Layout dem Backup ähnelt und keine Konfigurationsänderungen am Storage- und Datenbank-Stack durchgeführt wurden, erfolgt die Wiederherstellung direkt, wobei die Wiederherstellung von Datei oder LUN auf ONTAP durchgeführt wird. SnapCenter unterstützt als Teil der in-Place-Wiederherstellungsmethode nur Single File SnapRestore (SFSR).

Data ONTAP 8.3 oder höher unterstützt in-Place-Restores vom sekundären Standort.

Wenn Sie die Datenbank wiederherstellen möchten, stellen Sie sicher, dass nur Datendateien auf der ASM-Festplattengruppe vorhanden sind. Sie müssen ein Backup erstellen, nachdem Änderungen an der ASM-Laufwerksgruppe oder in der physischen Struktur der Datenbank vorgenommen wurden. Nach der Durchführung der in-Place-Wiederherstellung enthält die Festplattengruppe die gleiche Anzahl von Datendateien wie zum Zeitpunkt des Backups.

Die in-Place-Wiederherstellung wird automatisch angewendet, wenn die Laufwerksgruppe oder der Mount-Punkt den folgenden Kriterien entspricht:

- Nach dem Backup werden keine neuen Datendateien hinzugefügt (Prüfung für fremde Dateien)
- Kein Zusatz, Löschen oder Freizeit von ASM-Festplatte oder LUN nach Backup (ASM-Festplattengruppenstrukturüberprüfung)
- Keine Ergänzung, Löschung oder Wiederherstellung von LUNs zu LVM Disk Group (LVM Disk Group Strukturänderprüfung)

Sie können auch die Wiederherstellung an Ort und Stelle mit GUI, SnapCenter CLI oder PowerShell Cmdlet aktivieren, um die Prüfung der ausländischen Datei und die Strukturänderprüfung der LVM-Laufwerksgruppe zu überschreiben.

Durchführung einer in-Place-Wiederherstellung auf ASM RAC

In SnapCenter wird der Knoten, auf dem Sie wiederherstellen, als primärer Knoten und alle anderen Knoten des RAC bezeichnet, auf dem sich die ASM-Festplattengruppe befindet, als Peer-Nodes. SnapCenter ändert den Status der ASM-Laufwerksgruppe auf alle Nodes, in denen sich die ASM-Laufwerksgruppe im Mount-Zustand befindet, bevor sie die Speicherwiederherstellung durchführt. Nachdem die Speicherwiederherstellung abgeschlossen ist, ändert SnapCenter den Status der ASM-Laufwerksgruppe wie vor der Wiederherstellung.

In SAN-Umgebungen entfernt SnapCenter Geräte aus allen Peer-Nodes und führt LUN-Aufheben der Zuordnung durch, bevor der Storage wiederhergestellt wird. Nach der Storage-Wiederherstellung führt die

SnapCenter die LUN-Zuordnung durch und stellt Geräte auf allen Peer-Knoten wieder her. Wenn sich das Oracle RAC ASM-Layout in einer SAN-Umgebung auf LUNs befindet, führt die Wiederherstellung von SnapCenter LUN-Aufheben, LUN-Wiederherstellung und LUN-Map-Operationen auf allen Nodes des RAC-Clusters, in dem sich die ASM-Festplattengruppe befindet. Vor der Wiederherstellung auch dann, wenn alle Initiatoren der RAC-Nodes nicht für die LUNs verwendet wurden, erstellt nach dem Wiederherstellen von SnapCenter eine neue iGroup mit allen Initiatoren aller RAC-Nodes.

- Falls während der Vorratsspeicher-Aktivität auf Peer-Nodes ein Fehler auftritt, gibt SnapCenter den Status der ASM-Laufwerksgruppe automatisch wieder, so wie es zuvor war, bevor die Wiederherstellung auf Peer-Nodes durchgeführt wurde, auf denen der Vorspeichervorgang erfolgreich war. Rollback wird für den primären und den Peer-Knoten, auf dem der Vorgang fehlgeschlagen ist, nicht unterstützt. Bevor Sie eine andere Wiederherstellung versuchen, müssen Sie das Problem auf dem Peer-Node manuell beheben und die ASM-Laufwerksgruppe auf dem primären Node wieder in den Mount-Status versetzen.
- Falls 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 mit der Speicherwiederherstellung manuell beheben und die ASM-Laufwerksgruppe auf dem primären Knoten wieder in den Bereitstellungsstatus versetzen.
- Falls während der Speicherung auf einem der Peer-Nodes ein Fehler auftritt, wird SnapCenter mit dem Wiederherstellungsvorgang auf den anderen Peer-Nodes fortgesetzt. Sie müssen das Problem nach der Wiederherstellung manuell auf dem Peer-Node beheben.

Arten von Wiederherstellungsvorgängen, die für Oracle-Datenbanken unterstützt werden

SnapCenter ermöglicht Ihnen die Durchführung verschiedener Arten von Restore-Vorgängen für Oracle Datenbanken.

Vor dem Wiederherstellen der Datenbank werden Backups validiert, um festzustellen, ob Dateien im Vergleich zu den tatsächlichen Datenbankdateien fehlen.

Vollständige Wiederherstellung

- Stellt nur die Datendateien wieder her
- Stellt nur die Kontrolldateien wieder her
- Stellt die Datendateien und Kontrolldateien wieder her
- Stellt Datendateien, Kontrolldateien und Wiederherstellungsprotokolle in Data Guard Standby und Active Data Guard Standby-Datenbanken wieder her

Teilwiederherstellung

- Stellt nur die ausgewählten Tabellen wieder her
- Stellt nur die ausgewählten pluggable Datenbanken (PDBs) wieder her
- Stellt nur die ausgewählten Tabellen einer PDB wieder her

Arten von für Oracle-Datenbanken unterstützten Recovery-Vorgängen

SnapCenter ermöglicht Ihnen die Durchführung verschiedener Arten von Recovery-Vorgängen für Oracle Datenbanken.

- Die Datenbank bis zur letzten Transaktion (alle Logs)
- Die Datenbank bis zu einer bestimmten Systemänderungsnummer (SCN)

- Die Datenbank auf einem bestimmten Datum und einer bestimmten Uhrzeit aktualisiert

  Sie müssen Datum und Uhrzeit für die Recovery auf der Grundlage der Zeitzone des Datenbankhosts angeben.

  SnapCenter bietet auch die Option „kein Recovery“ für Oracle Datenbanken.

> Das Plug-in für Oracle-Datenbank unterstützt kein Recovery, wenn Sie mithilfe eines Backups wiederhergestellt haben, das mit der Datenbankrolle als Standby erstellt wurde. Sie müssen für physische Standby-Datenbanken immer ein manuelles Recovery durchführen.

Einschränkungen im Zusammenhang mit dem Restore und Recovery von Oracle Datenbanken

Bevor Sie Restore- und Recovery-Vorgänge durchführen, müssen Sie die Einschränkungen beachten.

Wenn Sie eine beliebige Oracle-Version von 11.2.0.4 bis 12.1 verwenden, 0.1 befindet sich der Wiederherstellungsvorgang im Status „Hung“, wenn Sie den Befehl „*renamedg*“ ausführen. Sie können den Oracle Patch 19544733 anwenden, um dieses Problem zu beheben.

Die folgenden Wiederherstellungs- und Recovery-Vorgänge werden nicht unterstützt:

- Restore und Recovery von Tabellen der Root-Container-Datenbank (CDB)
- Wiederherstellung temporärer Tabellen und temporärer Tablespaces im Zusammenhang mit PDBs
- Wiederherstellung und Wiederherstellung von Tabellen aus mehreren PDBs gleichzeitig
- Wiederherstellung von Log-Backups
- Wiederherstellung von Backups an einem anderen Speicherort
- Wiederherstellung von Wiederherstellungsprotokolldateien in einer anderen Konfiguration als Data Guard Standby oder Active Data Guard Standby-Datenbanken
- SPFILE und Password wiederherstellen
- Wenn Sie einen Wiederherstellungsvorgang für eine Datenbank durchführen, die mit dem bestehenden Datenbanknamen auf demselben Host neu erstellt wurde, von SnapCenter verwaltet wurde und über gültige Backups verfügte, überschreibt der Wiederherstellungsvorgang die neu erstellten Datenbankdateien, obwohl die DBIDs unterschiedlich sind.

  Dies kann durch die Durchführung einer der folgenden Maßnahmen vermieden werden:

  - Ermitteln Sie die SnapCenter Ressourcen, nachdem die Datenbank neu erstellt wurde
  - Erstellen Sie ein Backup der neu erstellten Datenbank

Einschränkungen im Zusammenhang mit der zeitpunktgenauen Recovery von Tablespaces

- Point-in-Time Recovery (PITR) von SYSTEM, SYSAUX und UNDO Tablespaces wird nicht unterstützt
- PITR der Tabellen können nicht zusammen mit anderen Arten von Restores ausgeführt werden
- Wenn ein Tablespace umbenannt wird und Sie ihn bis zu einem Punkt wiederherstellen möchten, bevor er umbenannt wurde, müssen Sie den früheren Namen des Tablespaces angeben
- Wenn die Tabellenbedingungen in einem Tablespace in einem anderen Tablespace enthalten sind, sollten Sie beide Tabellen wiederherstellen
- Wenn eine Tabelle und ihre Indizes in verschiedenen Tabellen gespeichert werden, sollten die Indizes vor

der Durchführung von PITR gelöscht werden

- PITR kann nicht verwendet werden, um den aktuellen Standardtablespaces wiederherzustellen
- PITR kann nicht verwendet werden, um Tabellen mit einem der folgenden Objekte wiederherzustellen:
  - Objekte mit zugrunde liegenden Objekten (z. B. materialisierte Ansichten) oder enthaltenen Objekten (z. B. partitionierte Tabellen), sofern sich nicht alle zugrunde liegenden oder enthaltenen Objekte im Wiederherstellungssatz befinden

    Wenn außerdem die Partitionen einer partitionierten Tabelle in verschiedenen Tabellen gespeichert werden, sollten Sie die Tabelle entweder vor der Durchführung von PITR ablegen oder alle Partitionen in denselben Tablespace verschieben, bevor Sie PITR ausführen.

  - Segmente rückgängig machen oder zurücksetzen
  - Oracle 8 kompatible erweiterte Warteschlangen mit mehreren Empfängern
  - Objekte, die dem SYS-Benutzer gehören

    Beispiele für diese Objekttypen sind PL/SQL, Java-Klassen, Ausrufprogramme, Ansichten, Synonyme, Benutzer, Berechtigungen, Abmessungen, Verzeichnisse und Sequenzen.

Quellen und Ziele für die Wiederherstellung von Oracle-Datenbanken

Sie können eine Oracle Datenbank aus einer Backup-Kopie auf dem Primär- oder Sekundärspeicher wiederherstellen. Sie können Datenbanken nur an demselben Speicherort auf derselben Datenbankinstanz wiederherstellen. Im Real Application Cluster (RAC) Setup können Sie jedoch Datenbanken auf anderen Knoten wiederherstellen.

Quellen für Wiederherstellungsvorgänge

Sie können Datenbanken aus einem Backup auf dem primären oder sekundären Storage wiederherstellen. Wenn Sie in einer Konfiguration mit mehreren Spiegelungen ein Backup auf dem sekundären Storage wiederherstellen möchten, können Sie die sekundäre Storage-Spiegelung als Quelle auswählen.

Ziele für Wiederherstellungen

Sie können Datenbanken nur an demselben Speicherort auf derselben Datenbankinstanz wiederherstellen.

In einem RAC Setup können Sie RAC-Datenbanken von jedem Knoten im Cluster wiederherstellen.

Vordefinierte Umgebungsvariablen zur Wiederherstellung spezifischer Vorschrift und Postscript

Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Prescript und das Postscript beim Wiederherstellen einer Datenbank ausführen.

Unterstützte vordefinierte Umgebungsvariablen für die Wiederherstellung 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 Datenbanknamen, die durch Pipe getrennt

sind.

Beispiel: NFSB31

- **SC_HOST** gibt den Hostnamen der Datenbank an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** gibt den Betriebssystembesitzer der Datenbank an.

  Beispiel: oracle

- **SC_OS_GROUP** gibt die Betriebssystemgruppe der Datenbank an.

  Beispiel: Oinstall

- **SC_BACKUP_NAME** gibt den Namen des Backups an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiele:

  - Wenn die Datenbank nicht im ARCHIVELOG-Modus ausgeführt wird: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 natürlich 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 Anwendungs-Volumes ausgefüllt.

  Beispiele:

  - Wenn die Datenbank nicht im ARCHIVELOG-Modus ausgeführt wird: DATEN@203 Paillette LOG@205
  - Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird: DATEN@203. PROTOKOLL@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 wiederhergestellten Dateien und auch den Wiederherstellungsumfang an.

  Beispiel: RESTORESCOPE:usingBackupControlfile=false natürlich ECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Informationen zu Trennzeichen finden Sie unter "Unterstützte Trennzeichen".

Anforderungen für die Wiederherstellung einer Oracle-Datenbank

Bevor Sie eine Oracle-Datenbank wiederherstellen, sollten Sie sicherstellen, dass die Voraussetzungen abgeschlossen sind.

- Sie sollten Ihre Restore- und Recovery-Strategie definiert haben.
- Der SnapCenter Administrator sollte Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren.
- Wenn Archivprotokolle im Rahmen der Datensicherung beschnitten werden, sollten Sie die erforderlichen Archiv-Log-Backups manuell gemountet haben.
- Wenn Sie Oracle Datenbanken wiederherstellen möchten, die sich auf einer Virtual Machine Disk (VMDK) befinden, sollten Sie sicherstellen, dass der Gastrechner die erforderliche Anzahl an freien Steckplätzen für die Zuweisung der geklonten VMDKs bietet.
- Sie sollten sicherstellen, dass alle Daten-Volumes und Archivprotokollvolumes der Datenbank geschützt sind, wenn für diese Datenbank ein sekundärer Schutz aktiviert ist.
- Sie sollten sicherstellen, dass sich die RAC One Node-Datenbank im Status „Nomount“ befindet, um die Steuerdatei oder die vollständige Datenbankwiederherstellung durchzuführen.
- Wenn Sie eine ASM-Datenbankinstanz in einer NFS-Umgebung haben, sollten Sie den ASM-Festplattenpfad */var/opt/snapcenter/scu/Clones/*/** in den im parameter asm_diskstring festgelegten Pfad hinzufügen, um die ASM-Protokoll-Backups erfolgreich im Rahmen des Wiederherstellungsvorgangs zu mounten.
- Im parameter asm_diskstring sollten Sie *AFD:** konfigurieren, wenn Sie ASMFD verwenden oder *ORCL:** konfigurieren, 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 bei _ € ORACLE_HOME/Network/admin_ für nicht-ASM-Datenbanken verfügbar ist, und _ € GRID_HOME/Network/admin_ für ASM-Datenbanken, wenn Sie die Betriebssystemauthentifizierung deaktiviert und die Oracle-Datenbankauthentifizierung für eine Oracle-Datenbank aktiviert haben, und die Datendateien und Kontrolldateien dieser Datenbank wiederherstellen möchten.
- Sie sollten den Wert des SCORestoreTimeout-Parameters erhöhen, indem Sie den Befehl Set-SmConfigSettings ausführen, wenn sich die Datenbankgröße in Terabyte (TB) befindet.
- Sie sollten sicherstellen, dass alle für vCenter erforderlichen Lizenzen installiert sind und auf dem neuesten Stand sind.

  Wenn die Lizenzen nicht installiert oder auf dem neuesten Stand sind, wird eine Warnmeldung angezeigt. Wenn Sie die Warnung ignorieren und fortfahren, schlägt die Wiederherstellung aus RDM fehl.

- Sie sollten sicherstellen, dass die LUN nicht dem AIX-Host mit iGroup zugeordnet ist, die aus gemischten Protokollen iSCSI und FC besteht. Weitere Informationen finden Sie unter "Der Vorgang schlägt fehl, da der Fehler nicht in der Lage ist, das Gerät für die LUN zu ermitteln".

Stellen Sie Oracle Datenbanken wieder her

Bei einem Datenverlust können Sie mit SnapCenter Daten von einem oder mehreren Backups auf Ihrem aktiven Dateisystem wiederherstellen und dann die Datenbank wiederherstellen.

Bevor Sie beginnen

Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript zuweisen.

Über diese Aufgabe

- Die Recovery wird anhand der Archivprotokolle durchgeführt, die am konfigurierten Speicherort für das Archivprotokoll 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 gemeinsam als archiviertes Redo-Protokoll bezeichnet werden. SnapCenter identifiziert und bindet die optimale Anzahl von Protokoll-Backups auf Basis der angegebenen SCN, des ausgewählten Datums und der ausgewählten Uhrzeit oder der Option „Protokolle“. Wenn die für die Recovery 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 ASM-Datenbank von ASMLIB zu ASMFD migrieren, können die mit ASMLIB erstellten Backups nicht zur Wiederherstellung der Datenbank verwendet werden. Sie sollten Backups in der ASMFD-Konfiguration erstellen und diese Backups für die Wiederherstellung verwenden. Wenn die ASM-Datenbank von ASMFD zu ASMLIB migriert wird, sollten Sie zur Wiederherstellung auch Backups in der ASMLIB-Konfiguration erstellen.

  Wenn Sie eine Datenbank wiederherstellen, wird auf dem Oracle-Datenbank-Host im Verzeichnis */var/opt/snapcenter/sco/lock* eine operative Sperrdatei (.sm_Lock_dbsid) erstellt, um zu vermeiden, dass mehrere Vorgänge in der Datenbank ausgeführt werden. Nach dem Wiederherstellen der Datenbank wird die operative Sperrdatei automatisch entfernt.

  Die Wiederherstellung der SPFILE- und Password-Datei wird nicht unterstützt.

- Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.

5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wenn Sie in einer RAC-Umgebung (Real Application Clusters) eine Sicherung einer Datenbank ausgewählt haben, wählen Sie den RAC-Knoten aus.
   b. Wenn Sie eine gespiegelte oder Vault-Daten auswählen:
      - Wenn keine Protokollsicherung bei Spiegel oder Tresor vorhanden ist, wird nichts ausgewählt und die Lokatoren leer sind.
      - Wenn Protokollsicherungen in Mirror oder Vault vorhanden sind, wird die neueste Protokollsicherung ausgewählt und der entsprechende Locator angezeigt.

      Wenn die ausgewählte Protokollsicherung sowohl im Spiegelungs- als auch im Tresorverzeichnis vorhanden ist, werden beide Lokatoren angezeigt.

   c. Führen Sie folgende Aktionen durch:

Sie möchten wiederherstellen…	**Tun Sie das…**
Alle Datendateien der Datenbank	Wählen Sie **Alle Datendateien**. Nur die Datendateien der Datenbank werden wiederhergestellt. Die Kontrolldateien, Archivprotokolle oder Wiederherstellungsprotokolle werden nicht wiederhergestellt.
Tablespaces	Wählen Sie **Tablespaces**. Sie können die Tabellen angeben, die Sie wiederherstellen möchten.
Kontrolldateien	Wählen Sie **Kontrolldateien** aus. Stellen Sie beim Wiederherstellen von Kontrolldateien sicher, dass die Verzeichnisstruktur entweder vorhanden ist oder mit dem korrekten Benutzer- und Gruppeneigentum erstellt werden soll, falls vorhanden, damit die Dateien durch den Wiederherstellungsvorgang an den Zielspeicherort kopiert werden können. Wenn das Verzeichnis nicht vorhanden ist, schlägt der Wiederherstellungsauftrag fehl.

Sie möchten wiederherstellen…	Tun Sie das…
Wiederholen Sie die Protokolldateien	Wählen Sie **Redo-Log-Dateien** aus. Diese Option ist nur für Data Guard Standby- oder Active Data Guard-Standby-Datenbanken verfügbar. Redo-Log-Dateien werden nicht für Datenbanken gesichert, die nicht von Data Guard stammen. Für Datenbanken, die nicht von Data Guard stammen, wird die Recovery mit Archivprotokollen durchgeführt.
Steckbare Datenbanken (PDBs)	Wählen Sie **Pluggable Databases** aus, und geben Sie dann die PDBs an, die Sie wiederherstellen möchten.
Steckbare Datenbank-Tabellen (PDB)	Wählen Sie **Pluggable Database (PDB) Tablespaces** aus, und geben Sie dann die PDB und die Tablespaces dieser PDB an, die Sie wiederherstellen möchten. Diese Option ist nur verfügbar, wenn Sie eine PDB für die Wiederherstellung ausgewählt haben.

d. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.

   Die verschiedenen Status einer Datenbank von höher bis niedriger sind offen, montiert, gestartet und heruntergefahren. Sie müssen dieses Kontrollkästchen aktivieren, wenn sich die Datenbank in einem höheren Zustand befindet, der Status jedoch in einen niedrigeren Zustand geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen. Wenn sich die Datenbank in einem niedrigeren Zustand befindet, aber der Status in einen höheren Zustand geändert werden muss, um den Wiederherstellungsvorgang auszuführen, wird der Datenbankstatus automatisch geändert, auch wenn Sie das Kontrollkästchen nicht aktivieren.

Wenn sich eine Datenbank im Status „offen“ befindet und die Datenbank für die Wiederherstellung im Status „angehängt“ befinden muss, wird der Datenbankzustand nur geändert, wenn Sie dieses Kontrollkästchen aktivieren.

a. Wählen Sie **erzwingen in place Restore** aus, wenn Sie in den Szenarien, in denen neue Datendateien nach dem Backup hinzugefügt werden, oder wenn LUNs zu einer LVM-Laufwerksgruppe hinzugefügt, gelöscht oder neu erstellt werden sollen, in-place-Wiederherstellung durchführen möchten.

7. Führen Sie auf der Seite „Recovery Scope“ die folgenden Aktionen durch:

Sie suchen…	Tun Sie das…
Möchten Sie die letzte Transaktion wiederherstellen	Wählen Sie **Alle Protokolle**.
Wiederherstellen einer bestimmten Systemänderungsnummer (SCN)	Wählen Sie **bis SCN (Systemänderungsnummer)**.
Möchten Sie Daten zu einer bestimmten Zeit wiederherstellen	Wählen Sie **Datum und Uhrzeit**. Sie müssen Datum und Uhrzeit der Zeitzone des Datenbank-Hosts angeben.
Möchten Sie nicht wiederherstellen	Wählen Sie **Keine Wiederherstellung**.
Soll beliebige externe Archiv-Log-Speicherorte angeben	Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird, identifiziert und montiert SnapCenter die optimale Anzahl von Protokoll-Backups basierend auf der angegebenen SCN, ausgewählten Datum und Uhrzeit oder allen Protokollen. Wenn Sie weiterhin den Speicherort der externen Archivprotokolldateien angeben möchten, wählen Sie **Externe Archivprotokolle angeben**. Wenn Archivprotokolle im Rahmen der Sicherung beschnitten werden und Sie die erforderlichen Archiv-Log-Backups manuell gemountet haben, müssen Sie den gemounteten Backup-Pfad als externen Archiv-Log-Speicherort für die Wiederherstellung angeben. Sie sollten den Pfad und den Inhalt des Mount-Pfads überprüfen, bevor Sie ihn als externen Speicherort des Protokolls auflisten. • "Oracle Datensicherung mit ONTAP" • "Der Vorgang schlägt mit ORA-00308-Fehler fehl"

Eine Wiederherstellung mit einer Recovery von sekundären Backups ist nicht möglich, wenn Archiv-Protokoll-Volumes nicht geschützt sind, aber Daten-Volumes gesichert sind. Sie können nur wiederherstellen, indem Sie **Keine Wiederherstellung**.

Wenn Sie eine RAC-Datenbank wiederherstellen, bei der die Option Open Database ausgewählt ist, wird nur die RAC-Instanz, in der der Wiederherstellungsvorgang initiiert wurde, wieder in den Status Open zurückgebracht.

Die Recovery wird nicht für Data Guard Standby- und Active Data Guard-Standby-Datenbanken unterstützt.

8. Geben Sie auf der Seite PreOps den Pfad und die Argumente des Preskript ein, das Sie vor der Wiederherstellung ausführen möchten.

   Sie müssen die Voreinstellungen entweder im Pfad */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

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

   Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Skript und das Postscript ausführen. "Weitere Informationen ."

9. Führen Sie auf der Seite PostOps die folgenden Schritte aus:

   a. Geben Sie den Pfad und die Argumente des Postscript ein, das Sie nach der Wiederherstellung ausführen möchten.

      Sie müssen die Postskripte entweder in */var/opt/snapcenter/spl/scripts* oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

      ⓘ Wenn der Wiederherstellungsvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungstätigkeiten werden direkt ausgelöst.

   b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

      Nach dem Wiederherstellen einer Container-Datenbank (CDB) mit oder ohne Kontrolldateien oder nach dem Wiederherstellen nur CDB-Kontrolldateien, wenn Sie angeben, die Datenbank nach der Wiederherstellung zu öffnen, dann wird nur die CDB geöffnet und nicht die steckbaren Datenbanken (PDB) in dieser CDB.

      In einem RAC-Setup wird nach der Wiederherstellung nur die RAC-Instanz geöffnet, die für die Wiederherstellung verwendet wird.

      ⓘ Nach dem Wiederherstellen eines Benutzertablespaces mit Steuerdateien, eines Systemtablespaces mit oder ohne Steuerdateien oder einer PDB mit oder ohne Steuerdateien wird nur der Status der PDB, die mit dem Wiederherstellungsvorgang in Verbindung steht, in den ursprünglichen Zustand geändert. Der Zustand der anderen PDBs, die nicht für die Wiederherstellung verwendet wurden, wird nicht in den ursprünglichen Zustand geändert, weil der Zustand dieser PDBs nicht gespeichert wurden. Sie müssen manuell den Status der PDBs ändern, die nicht für die Wiederherstellung verwendet wurden.

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

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

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

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

Für weitere Informationen

- "Oracle RAC One-Knoten-Datenbank wird zur Durchführung von SnapCenter-Operationen übersprungen"
- "Fehler beim Wiederherstellen von einem sekundären SnapMirror- oder SnapVault-Standort"
- "Wiederherstellung aus einem Backup einer verwaisten Inkarnation fehlgeschlagen"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Wiederherstellen von Tabellen mit Point-in-Time Recovery

Sie können einen bestimmten Satz von Tablespaces wiederherstellen, die beschädigt oder verworfen wurden, ohne dass die anderen Tabellen der Datenbank beeinträchtigt werden. SnapCenter verwendet RMAN für die Durchführung des Point-in-Time Recovery (PITR) der Tabellen.

Bevor Sie beginnen

- Die Backups, die zur Durchführung von PITR von Tabellen erforderlich sind, sollten katalogisiert und gemountet werden.
- Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript zuweisen.

Über diese Aufgabe

Während des PITR-Betriebs erstellt RMAN eine Zusatzinstanz am angegebenen Hilfsziel. Das Hilfeziel kann ein Bereitstellungspunkt oder eine ASM-Laufwerksgruppe sein. Wenn genügend Speicherplatz am Einbauort vorhanden ist, können Sie eine der montierten Positionen anstelle eines dedizierten Mount-Punkts wiederverwenden.

Geben Sie Datum und Uhrzeit oder SCN an, und der Tablespace wird in der Quelldatenbank wiederhergestellt.

Sie können mehrere Tabellen mit ASM, NFS und SAN-Umgebungen auswählen und wiederherstellen. Wenn sich beispielsweise Tablespaces TS2 und TS3 auf NFS und TS4 im SAN befinden, können Sie alle Tabellen wiederherstellen.

In einem RAC-Setup können Sie PITR von Tablespaces von jedem Knoten des RAC ausführen.

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank des Typs Single Instance (mandantenfähig) aus der Detailansicht der Datenbank oder in der Detailansicht der Ressourcengruppen aus.

Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.

   Wenn die Sicherung nicht katalogisiert ist, sollten Sie die Sicherung auswählen und auf **Katalog** klicken.

5. Wählen Sie die katalogisierte Sicherung aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wenn Sie in einer RAC-Umgebung (Real Application Clusters) eine Sicherung einer Datenbank ausgewählt haben, wählen Sie den RAC-Knoten aus.
   b. Wählen Sie **Tablespaces** aus, und legen Sie dann die Tablespaces fest, die Sie wiederherstellen möchten.

      PITR kann auf SYSAUX, SYSTEM und TABLESPACES nicht ausgeführt werden.

   c. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.
7. Führen Sie auf der Seite „Wiederherstellungsumfang“ eine der folgenden Aktionen durch:
   - Wenn Sie eine bestimmte Systemänderungsnummer (SCN) wiederherstellen möchten, wählen Sie **bis SCN** und geben Sie das SCN und das Hilfeziel an.
   - Wenn Sie ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten, wählen Sie **Datum und Uhrzeit** und geben Sie Datum und Uhrzeit sowie das Hilfsziel an.

     SnapCenter identifiziert und katalogisiert die optimale Anzahl von Daten- und Protokollierungs-Backups, die für die Durchführung von PITR auf der Grundlage des angegebenen SCN oder des ausgewählten Datums und der ausgewählten Zeit erforderlich sind.
8. Geben Sie auf der Seite PreOps den Pfad und die Argumente des Preskript ein, das Sie vor der Wiederherstellung ausführen möchten.

   Sie sollten die Voreinstellungen entweder im Pfad /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig wird der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

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

   Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Skript und das Postscript ausführen. "Weitere Informationen ."
9. Führen Sie auf der Seite PostOps die folgenden Schritte aus:
   a. Geben Sie den Pfad und die Argumente des Postscript ein, das Sie nach der Wiederherstellung ausführen möchten.

      Wenn der Wiederherstellungsvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungstätigkeiten werden direkt ausgelöst.

   b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen

möchten.

10. Wählen Sie auf der Seite Benachrichtigung aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Wiederherstellen steckbarer Datenbanken über zeitpunktgenaues Recovery

Sie können eine steckbare Datenbank (PDB) wiederherstellen, die beschädigt oder verworfen wurde, ohne die andere DBs in der Container-Datenbank (CDB) zu belasten. SnapCenter nutzt RMAN für die Durchführung von Point-in-Time Recoverys (PITR) der PDB.

Bevor Sie beginnen

- Die Backups, die für die PITR einer PDB benötigt werden, sollten katalogisiert und gemountet werden.

  In einem RAC-Setup sollten Sie die PDB manuell schließen (ändern des Status in „MOUNT“) auf allen Knoten des RAC-Setups.

- Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript zuweisen.

Über diese Aufgabe

Während des PITR-Betriebs erstellt RMAN eine Zusatzinstanz am angegebenen Hilfsziel. Das Hilfeziel kann ein Bereitstellungspunkt oder eine ASM-Laufwerksgruppe sein. Wenn genügend Speicherplatz am Einbauort vorhanden ist, können Sie eine der montierten Positionen anstelle eines dedizierten Mount-Punkts wiederverwenden.

Sie sollten das Datum und die Uhrzeit oder das SCN angeben, um PITR der PDB durchzuführen. RMAN kann LESE-, SCHREIBSCHUTZ- ODER abfallende PDBs einschließlich Datendateien wiederherstellen.

Sie können nur Folgendes wiederherstellen:

- Jeweils eine PDB
- Ein Tablespace in einer PDB
- Mehrere Tabellen derselben PDB

In einem RAC-Setup können Sie PITR von Tablespaces von jedem Knoten des RAC ausführen.

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank des Typs Single Instance (mandantenfähig) aus der Detailansicht der Datenbank oder in der Detailansicht der Ressourcengruppen aus.

Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.

   Wenn die Sicherung nicht katalogisiert ist, sollten Sie die Sicherung auswählen und auf **Katalog** klicken.

5. Wählen Sie die katalogisierte Sicherung aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wenn Sie in einer RAC-Umgebung (Real Application Clusters) eine Sicherung einer Datenbank ausgewählt haben, wählen Sie den RAC-Knoten aus.
   b. Je nachdem, ob Sie die PDB oder Tablespaces in einer PDB wiederherstellen möchten, führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Schritte…
PDB wiederherstellen	i. Wählen Sie **Pluggable Databases (PDBs)** aus. ii. Geben Sie die PDB an, die wiederhergestellt werden soll. Sie können PITR nicht in der PDB-Datenbank mit Wert für „PITR“ ausführen.
Tablespaces in einer PDB wiederherstellen	i. Wählen Sie die Tabellen * Pluggable Database (PDB)* aus. ii. Geben Sie den PDB an. iii. Geben Sie entweder einen einzelnen Tablespace oder mehrere Tablespaces an, die Sie wiederherstellen möchten. PITR kann auf SYSAUX, SYSTEM und TABLESPACES nicht ausgeführt werden.

   c. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.
7. Führen Sie auf der Seite „Wiederherstellungsumfang“ eine der folgenden Aktionen durch:
   - Wenn Sie eine bestimmte Systemänderungsnummer (SCN) wiederherstellen möchten, wählen Sie **bis SCN** und geben Sie das SCN und das Hilfeziel an.
   - Wenn Sie ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten, wählen Sie **Datum und Uhrzeit** und geben Sie Datum und Uhrzeit sowie das Hilfsziel an.

     SnapCenter identifiziert und katalogisiert die optimale Anzahl von Daten- und Protokollierungs-

Backups, die für die Durchführung von PITR auf der Grundlage des angegebenen SCN oder des ausgewählten Datums und der ausgewählten Zeit erforderlich sind.

8. Geben Sie auf der Seite PreOps den Pfad und die Argumente des Preskript ein, das Sie vor der Wiederherstellung ausführen möchten.

   Sie sollten die Voreinstellungen entweder im Pfad /var/opt/snapcenter/spl/scripts oder in einem beliebigen Ordner in diesem Pfad speichern. Standardmäßig wird der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie Ordner in diesem Pfad erstellt haben, um die Skripte zu speichern, müssen Sie diese Ordner im Pfad angeben.

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

   Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Skript und das Postscript ausführen. "Weitere Informationen ."

9. Führen Sie auf der Seite PostOps die folgenden Schritte aus:
   a. Geben Sie den Pfad und die Argumente des Postscript ein, das Sie nach der Wiederherstellung ausführen möchten.

      Wenn der Wiederherstellungsvorgang fehlschlägt, werden Postscripts nicht ausgeführt und Bereinigungstätigkeiten werden 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 Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.
11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Stellen Sie Oracle Datenbanken mithilfe von UNIX-Befehlen wieder her

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore- und Recovery-Vorgängen und Monitoring der betrieblichen Vorgänge.

Über diese Aufgabe

- Sie sollten die folgenden Befehle ausführen, um die Verbindung zum SnapCenter-Server herzustellen, die Backups aufzulisten, seine Informationen abzurufen und die Sicherung wiederherzustellen.

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

- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer: *Open-SmConnection*
2. Rufen Sie die Informationen über die Backups 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 zum Backup einer bestimmten Ressource mit einer bestimmten Backup-ID ab. Die Informationen umfassen Datenbanknamen, Version, Home, SCN starten und beenden, Tabellen, steckbare Datenbanken und deren Tabellen.

4. Stellen Sie Daten aus dem Backup wieder her: *Restore-SmBackup*

Überwachen Sie die Restore-Vorgänge für Oracle Datenbanken

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

Über diese Aufgabe

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

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

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

Schritte

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

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

Wiederherstellungsvorgänge für Oracle-Datenbank abbrechen

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Nachdem Sie den Wiederherstellungsvorgang gestartet haben, klicken Sie auf das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Oracle Datenbank klonen

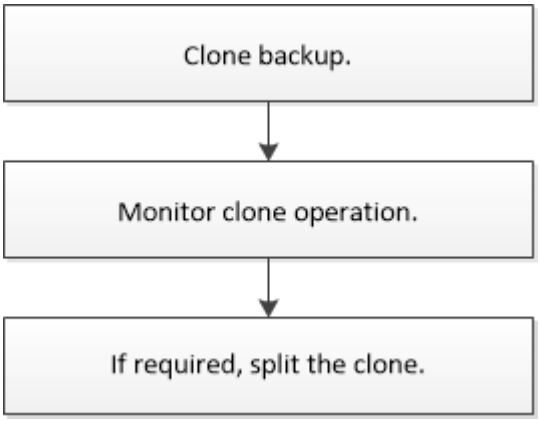
Klon-Workflow

Der Klon-Workflow umfasst die Planung, die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Sie können Datenbanken aus den folgenden Gründen klonen:

- Funktionen zu testen, die während der Applikationsentwicklungszyklen mit der aktuellen Datenbankstruktur und Inhalten implementiert werden müssen.
- Um Data Warehouses mit Tools zur Datenextraktion und -Bearbeitung zu befüllen.
- Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden.

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Klonstrategie für Oracle Datenbanken definieren

Eine Strategie vor dem Klonen Ihrer Datenbank definieren, um sicherzustellen, dass der Klonvorgang erfolgreich ist.

Arten von Backups, die zum Klonen unterstützt werden

SnapCenter unterstützt das Klonen verschiedener Backup-Typen von Oracle Datenbanken.

- Online Daten-Backup
- Online-Vollbackup
- Backup für Offline-Mounten
- Offline-Herunterfahren-Backup
- Backups von Data Guard Standby-Datenbanken und Active Data Guard Standby-Datenbanken
- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer RAC-Konfiguration (Real Application Clusters)
- Online-Daten-Backups, vollständige Online-Backups, Offline-Mount-Backups und Offline-Shutdown-Backups in einer ASM-Konfiguration (Automatic Storage Management)

SAN-Konfigurationen werden nicht unterstützt, wenn die Option „user_friendly_Names“ in der Multipath-Konfigurationsdatei auf „yes“ gesetzt ist.

Das Klonen von Backups für Archivprotokolle wird nicht unterstützt.

Arten von unterstützten Klonen für Oracle-Datenbanken

In einer Oracle Datenbankumgebung unterstützt SnapCenter das Klonen eines Datenbank-Backups. Sie können das Backup aus primären und sekundären Storage-Systemen klonen.

Der SnapCenter Server klont mit NetApp FlexClone Technologie Backups.

Sie können einen Klon aktualisieren, indem Sie den Befehl „Refresh-SmClone“ ausführen. Mit diesem Befehl wird ein Backup der Datenbank erstellt, der vorhandene Klon gelöscht und ein Klon mit demselben Namen erstellt.

Die Klonaktualisierung kann nur mit den UNIX Befehlen ausgeführt werden.

Namenskonventionen für Klone für Oracle Datenbanken

Von SnapCenter 3.0 unterscheidet sich die Namenskonvention für Klone von Dateisystemen von den Klonen von ASM-Festplattengruppen.

- Die Namenskonvention für SAN oder NFS-File-Systeme ist FileSystemNamesourceDatabase_CLONESID.
- Die Namenskonvention für ASM-Festplattengruppen ist SC_HASHCODEofDISKGROUP_CLONESID.

  HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Laufwerksgruppe eindeutig ist.

Einschränkungen beim Klonen von Oracle Datenbanken

Die Einschränkungen von Klonvorgängen sollten Sie beachten, bevor Sie die Datenbanken klonen.

- Wenn Sie eine Oracle-Version von 11.2.0.4 bis 12.1.0.1 verwenden, befindet sich der Klonvorgang im Status „Hung“, wenn Sie den Befehl „*renamedg*“ ausführen. Sie können den Oracle Patch 19544733 anwenden, um dieses Problem zu beheben.
- Das Klonen von Datenbanken aus einem LUN, die direkt an einen Host angebunden ist (z. B. durch die Verwendung von Microsoft iSCSI Initiator auf einem Windows Host), wird auf demselben Windows Host oder einem anderen Windows Host oder umgekehrt nicht unterstützt.
- Das Stammverzeichnis des Volume-Bereitstellungspunkts kann kein freigegebenes Verzeichnis sein.
- Wenn Sie eine LUN verschieben, die einen Klon in ein neues Volume enthält, kann der Klon nicht gelöscht werden.

Vordefinierte Umgebungsvariablen für das Klonen spezifischer Prescript und Postscript

Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Prescript und das Postscript beim Klonen einer Datenbank ausführen.

Unterstützte vordefinierte Umgebungsvariablen zum Klonen einer Datenbank

- **SC_ORIGINAL_SID** gibt die SID der Quelldatenbank an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: NFSB32

- **SC_ORIGINAL_HOST** gibt den Namen des Quellhosts an.

  Dieser Parameter wird für Anwendungs-Volumes 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 des Backups an.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiele:

  - Wenn die Datenbank nicht im ARCHIVELOG-Modus ausgeführt wird: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 natürlich 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 LOGBUCH: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 natürlich AV2

- **SC_ORIGINAL_OS_USER** gibt den Betriebssystembesitzer der Quelldatenbank an.

  Beispiel: oracle

- **SC_ORIGINAL_OS_GROUP** gibt die Betriebssystemgruppe der Quelldatenbank an.

  Beispiel: Oinstall

- **SC_TARGET_SID**" gibt die SID der geklonten Datenbank an.

  Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: Clonedb

- **SC_TARGET_HOST** gibt den Namen des Hosts an, auf dem die Datenbank geklont wird.

  Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

  Beispiel: asmrac1.gdl.englab.netapp.com

- **SC_TARGET_OS_USER** gibt den Betriebssystembesitzer der geklonten Datenbank an.

  Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

  Beispiel: oracle

- **SC_TARGET_OS_GROUP** gibt die Betriebssystemgruppe der geklonten Datenbank an.

  Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

  Beispiel: Oinstall

- **SC_TARGET_DB_PORT** gibt den Datenbank-Port der geklonten Datenbank an.

  Bei PDB-Klon-Workflow ist der Wert dieses Parameters nicht vordefiniert.

  Beispiel: 1521

Informationen zu Trennzeichen finden Sie unter "Unterstützte Trennzeichen".

Anforderungen für das Klonen einer Oracle Datenbank

Bevor Sie eine Oracle-Datenbank klonen, sollten Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

- Sie sollten eine Sicherung der Datenbank mit SnapCenter erstellt haben.

  Sie sollten erfolgreich Online-Daten erstellen und Backups oder Offline-Backups (Mounten oder Herunterfahren) protokollieren, damit der Klonvorgang erfolgreich abgeschlossen wurde.

- Wenn Sie die Steuerdatei oder die Pfade für die Wiederherstellungsprotokolle anpassen möchten, sollten Sie die erforderliche Dateisystemgruppe oder die automatische Speicherverwaltung (ASM) vorbereitgestellt haben.

  Standardmäßig werden Wiederherstellungsprotokolle und Kontrolldateien der geklonten Datenbank auf der ASM-Festplattengruppe oder auf 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:** konfigurieren, 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 folgende Anforderungen erfüllen:
  - Das SnapCenter Plug-in für Oracle Database sollte auf dem alternativen Host installiert sein.
  - Der Klon-Host sollte LUNs vom primären oder sekundären Storage erkennen können.
    - Wenn Sie vom primären Storage oder sekundären Storage (Vault oder Mirror) in einem alternativen Host klonen, stellen Sie sicher, dass eine iSCSI-Sitzung zwischen dem sekundären Storage und dem alternativen Host aufgebaut ist oder richtig für FC abgegrenzt wird.
    - Wenn Sie von Vault oder Mirror Storage auf demselben Host klonen, stellen Sie sicher, dass eine iSCSI-Sitzung zwischen dem Vault- oder Mirror-Storage und dem Host eingerichtet oder richtig für FC abgegrenzt wird.
    - Wenn Sie in einer virtualisierten Umgebung klonen, stellen Sie sicher, dass entweder eine iSCSI-

Sitzung zwischen dem primären oder sekundären Storage und dem ESX-Server, der den alternativen Host hostet, eingerichtet oder ordnungsgemäß für FC.

Weitere Informationen finden Sie unter "Dokumentation zu Host Utilities".

- Wenn die Quelldatenbank eine ASM-Datenbank ist:
  - Die ASM-Instanz sollte auf dem Host ausgeführt werden, auf dem der Klon ausgeführt wird.
  - Die ASM-Laufwerksgruppe sollte vor dem Klonvorgang bereitgestellt werden, wenn Sie Archivprotokolldateien der geklonten Datenbank in eine dedizierte ASM-Laufwerksgruppe platzieren möchten.
  - Der Name der Datendisk-Gruppe kann konfiguriert werden, aber stellen Sie sicher, dass der Name nicht von einer anderen ASM-Laufwerksgruppe auf dem Host verwendet wird, auf dem der Klon ausgeführt wird.

    Datendateien auf der ASM-Festplattengruppe werden als Teil des SnapCenter-Klon-Workflows bereitgestellt.
- Für NVMe sollte NVMe util installiert werden

- Der Schutztyp für die Daten-LUN und die Protokoll-LUN, wie Spiegel, Vault oder Mirror-Vault, sollte der gleiche sein, um beim Klonen zu einem alternativen Host mithilfe von Protokoll-Backups sekundäre Lokatoren zu erkennen.
- Sie sollten den Wert exclude_Seed_cdb_view in der Parameterdatei der Quelldatenbank auf FALSE setzen, um Informationen zum Klonen einer Sicherung von 12_c_-Datenbank abzurufen.

  Die SEED-PDB ist eine vom System bereitgestellte Vorlage, mit der die CDB PDBs erstellen kann. Die Samen-PDB wird PDB als Samen bezeichnet. Informationen zu PDB-Dollar finden Sie im Oracle Doc 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 die Mount-Punkte der Daten nicht unter der Wurzel des Mount-Punkts von Autofs liegen, da der Root-Benutzer des Plug-in-Hosts keine Berechtigung hat, Verzeichnisse unter dem Stammverzeichnis des Autofs Mount-Punkts zu erstellen.

  Wenn sich Kontroll- und Wiederherstellungsprotokolle unter dem Dateneinhängungspunkt befinden, sollten Sie den Pfad der Kontrolldatei ändern und anschließend den Dateipfad wiederholen.

  Sie können die neuen geklonten Mount-Punkte manuell mit dem Autofs-Subsystem registrieren. Die neuen geklonten Mount-Punkte werden nicht automatisch registriert.

- Wenn Sie ein TDE (Auto Login) haben und die Datenbank auf demselben oder einem anderen Host klonen möchten, sollten Sie 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 setzen und den lvm2-lvmetad-Service beenden, um erfolgreich ein Klonen in SAN-Umgebungen (Storage Area Network) unter Oracle Linux 7 oder höher oder Red hat Enterprise Linux (RHEL) 7 oder höher 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 mit einem NID-Skript geändert wird.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen

Aggregate der Storage Virtual Machine (SVM) befinden.

- Wenn bei NVMe ein Zielport von der Verbindung ausgeschlossen werden muss, sollten Sie den Zielknotennamen 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 dem AIX-Host mit iGroup zugeordnet ist, die aus gemischten Protokollen iSCSI und FC besteht. Weitere Informationen finden Sie unter "Der Vorgang schlägt fehl, da der Fehler nicht in der Lage ist, das Gerät für die LUN zu ermitteln".

Klonen eines Backups einer Oracle Datenbank

Sie können SnapCenter verwenden, um eine Oracle Datenbank mithilfe des Backups der Datenbank zu klonen.

Bevor Sie beginnen

Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript zuweisen.

Über diese Aufgabe

- Der Klonvorgang erstellt eine Kopie der Datenbankdatendateien und erstellt neue Online-Protokolldateien für die Wiederherstellung sowie Kontrolldateien. Die Datenbank kann auf Basis der angegebenen Wiederherstellungsoptionen optional bis zu einem bestimmten Zeitpunkt wiederhergestellt werden.

  Das Klonen schlägt fehl, wenn Sie versuchen, ein Backup zu klonen, das auf einem Linux Host auf einem AIX Host erstellt wurde, oder umgekehrt.

  SnapCenter erstellt eine Standalone-Datenbank, wenn sie aus einem Backup einer Oracle RAC Datenbank geklont wird. SnapCenter unterstützt die Erstellung von Klonen aus der Backup von Data Guard Standby und Active Data Guard Standby Datenbanken.

  Während des Klonens montierte SnapCenter die optimale Anzahl von Protokoll-Backups auf Basis von SCN oder dat und die Zeit für Recovery-Vorgänge. Nach der Wiederherstellung wird die Protokollsicherung abgehängt. Alle diese Klone sind unter */var/opt/snapcenter/scu/Clones/* eingebunden. 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 eines Backups einer ASM-Datenbank in einer SAN-Umgebung werden udev-Regeln für die geklonten Host-Geräte unter */etc/udev/rules.d/999-scu-netapp.rules* erstellt. Diese udev-Regeln, die den geklonten Host-Geräten zugeordnet sind, werden beim Löschen des Klons gelöscht.

  In einem Flex ASM-Setup können Sie keinen Klonvorgang auf Leaf-Knoten ausführen, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist.

- Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

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 Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

   Die Seite der Datenbanktopologie wird angezeigt.
4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (sekundär) aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite Name eine der folgenden Aktionen durch:

Ihr Ziel ist	Schritte…
Klonen einer Datenbank (CDB oder nicht-CDB)	a. Geben Sie die SID des Klons an. Der Clone SID ist standardmäßig nicht verfügbar, und die maximale Länge der SID beträgt 8 Zeichen. Sie sollten sicherstellen, dass auf dem Host, auf dem der Klon erstellt wird, keine Datenbank mit derselben SID vorhanden ist.
Klonen einer Plug-in-Datenbank (PDB)	a. Wählen Sie **PDB Clone**. b. Geben Sie die PDB an, die Sie klonen möchten. c. Geben Sie den Namen der geklonten PDB an. Detaillierte Schritte zum Klonen einer PDB finden Sie unter "Klonen einer sofort anschließbaren Datenbank".

   Wenn Sie eine gespiegelte oder Vault-Daten auswählen:

   - Wenn keine Protokollsicherung bei Spiegel oder Tresor vorhanden ist, wird nichts ausgewählt und die Lokatoren leer sind.
   - Wenn Protokollsicherungen in Mirror oder Vault vorhanden sind, wird die neueste Protokollsicherung ausgewählt und der entsprechende Locator angezeigt.

Wenn die ausgewählte Protokollsicherung sowohl im Spiegelungs- als auch im Tresorverzeichnis vorhanden ist, werden beide Lokatoren angezeigt.

7. Führen Sie auf der Seite Speicherorte die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonhost	Standardmäßig wird der Quell-Datenbank-Host befüllt. Wenn Sie den Klon auf einem anderen Host erstellen möchten, wählen Sie den Host aus, der dieselbe Version von Oracle und dasselbe Betriebssystem wie der des Quelldatenbankhosts hat.
Datendateiorte	Standardmäßig wird der Speicherort der Datendatei gefüllt. Die standardmäßige Namenskonvention von SnapCenter für SAN- oder NFS-File-Systeme ist FileSystemNamesourceDatabase_CLONESID. Die standardmäßige SnapCenter-Namenskonvention für ASM-Festplattengruppen ist SC_HASHCODEofDISKGROUP_CLONESID. Die HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Laufwerksgruppe eindeutig ist. Wenn Sie den Namen der ASM-Laufwerksgruppe anpassen, stellen Sie sicher, dass die Namenslänge die von Oracle unterstützte maximale Länge erfüllt. Wenn Sie einen anderen Pfad angeben möchten, müssen Sie die Mount-Punkte für Datendatei oder die Namen der ASM-Festplattengruppen für die Klondatenbank eingeben. Wenn Sie den Datenpfad anpassen, müssen Sie auch die Steuerdatei und die Redo-Log-Datei ASM-Festplattengruppennamen oder Dateisystem entweder auf den gleichen Namen für Datendateien oder auf ein vorhandenes ASM-Laufwerksgruppen oder Dateisystem ändern.

Für dieses Feld…	Tun Sie das…
Kontrolldateien	Standardmäßig wird der Pfad der Kontrolldatei ausgefüllt. Die Steuerdateien werden in derselben ASM-Laufwerksgruppe oder in demselben Dateisystem wie die der Datendateien abgelegt. Wenn Sie den Pfad der Steuerdatei überschreiben möchten, können Sie einen anderen Pfad für die Steuerdatei angeben. ⓘ Das Dateisystem oder die ASM-Laufwerksgruppe sollte auf dem Host vorhanden sein. Standardmäßig ist die Anzahl der Kontrolldateien mit der der Quelldatenbank identisch. Sie können die Anzahl der Kontrolldateien ändern, aber zum Klonen der Datenbank ist mindestens eine Kontrolldatei erforderlich. Sie können den Pfad der Steuerdatei an ein anderes Dateisystem (vorhanden) anpassen als den der Quelldatenbank.

Für dieses Feld…	Tun Sie das…
Wiederherstellungsprotokolle	Standardmäßig werden die Gruppe, der Pfad und ihre Größe der Wiederherstellungsprotokolle ausgefüllt. Die Wiederherstellungsprotokolle werden in derselben ASM-Festplattengruppe oder demselben Filesystem wie die Datendateien der geklonten Datenbank platziert. Wenn Sie den Pfad für die Wiederherstellungsprotokoll-Datei überschreiben möchten, können Sie den Pfad für die Wiederherstellungsprotokolle auf ein anderes Dateisystem als den der Quelldatenbank anpassen. Auf dem Host sollte das neue Dateisystem oder die ASM-Laufwerksgruppe vorhanden sein. Standardmäßig ist die Anzahl der Wiederherstellungsprotokolle, der Wiederherstellungsprotokolle und ihrer Größe mit der Quelldatenbank identisch. Sie können die folgenden Parameter ändern: • Anzahl der Wiederherstellungsprotokolle Zum Klonen der Datenbank sind mindestens zwei Wiederherstellungsprotokolle erforderlich. • Wiederholen Sie die Protokolldateien in jeder Gruppe und ihrem Pfad Sie können den Pfad der Redo-Log-Datei an ein anderes (vorhandenes) Dateisystem anpassen als den der Quelldatenbank. In der Gruppe für Wiederherstellungsprotokolle ist mindestens eine Wiederherstellungsprotokoll-Datei erforderlich, um die Datenbank zu klonen. • Größe der Wiederherstellungsprotokolldatei

8. Führen Sie auf der Seite Anmeldeinformationen die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Anmeldeinformationsname für sys-Benutzer	Wählen Sie das Credential aus, das zum Definieren des sys-Benutzerpassworts der Clone-Datenbank verwendet werden soll. Wenn SQLNET.AUTHENTICATION_SERVICES in sqlnet.ora-Datei auf dem Ziel-Host auf KEINE gesetzt ist, sollten Sie in der SnapCenter-GUI nicht **kein** als Credential auswählen.
Benutzername für die ASM-Instanz	Wählen Sie **Keine** aus, wenn die OS-Authentifizierung für die Verbindung zur ASM-Instanz auf dem Clone-Host aktiviert ist. Wählen Sie andernfalls die Oracle ASM-Berechtigung aus, die entweder mit „`sys`“-Benutzer oder mit einem Benutzer mit der Berechtigung `sysasm`“ für den Klon-Host konfiguriert ist.

Die Oracle-Startseite, der Benutzername und die Gruppendetails werden automatisch aus der Quelldatenbank ausgefüllt. 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 für das Prescript ein, das Sie vor dem Klonvorgang ausführen möchten.

      Sie müssen das Prescript entweder in */var/opt/snapcenter/spl/scripts* oder in einem Ordner in diesem Pfad speichern. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird.

      Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Skript und das Postscript ausführen. "Weitere Informationen ."

   b. Ändern Sie im Abschnitt Datenbankparameter-Einstellungen die Werte vorausgefüllter Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.

      Sie können weitere Parameter hinzufügen, indem Sie auf * * klicken  .

      Wenn Sie Oracle Standard Edition verwenden und die Datenbank im Archiv-Log-Modus ausgeführt wird oder Sie eine Datenbank aus dem Wiederherstellungsprotokoll wiederherstellen möchten, fügen Sie die Parameter hinzu und geben den Pfad an.

      - LOG_ARCHIVE_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

      > Der fast Recovery Area (FRA) ist in den vorausgefüllten Datenbankparametern nicht definiert. Sie können FRA konfigurieren, indem Sie die zugehörigen Parameter hinzufügen.

Der Standardwert von log_Archive_dest_1 liegt bei „€ORACLE_HOME/Clone_sid“ und an diesem Ort werden die Archivprotokolle der geklonten Datenbank 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 Laufwerksgruppe vorhanden sein und auf dem Host verfügbar gemacht werden soll.

a. Klicken Sie auf **Zurücksetzen**, um die Standardeinstellungen für die Datenbankparameter anzuzeigen.

10. Auf der PostOps Seite werden **Recover Database** und **Until Cancel** standardmäßig ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

    SnapCenter führt eine Recovery durch, indem das letzte Protokoll-Backup montiert wird, bei dem die nicht unterbrochene Sequenz von Archivprotokollen nach dem Daten-Backup zum Klonen ausgewählt wurde. Das Protokoll und das Daten-Backup sollten sich auf dem Primärspeicher befinden, um den Klon im Primärspeicher durchzuführen und Protokoll- und Daten-Backups auf dem Sekundärspeicher zu erstellen, um den Klon im Sekundärspeicher durchzuführen.

    Die Optionen **Recover Database** und **bis Abbrechen** sind nicht ausgewählt, wenn SnapCenter die entsprechenden Log-Backups nicht findet. Sie können den externen Archiv-Log-Speicherort angeben, wenn die Protokollsicherung in **externen Archiv-Log-Speicherorten angeben** nicht verfügbar ist. Sie können mehrere Protokollpositionen 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 die Quelldatenbank Data Guard Standby oder eine Active Data Guard Standby-Datenbank ist. Für Data Guard Standby oder eine Active Data Guard Standby-Datenbank bietet SnapCenter keine Option, um den Typ der Wiederherstellung in der SnapCenter GUI auszuwählen, aber die Datenbank wird mit bis Abbrechen Recovery-Typ wiederhergestellt, ohne Protokolle anzuwenden.

Feldname	Beschreibung
Bis Abbrechen	SnapCenter führt eine Recovery durch, indem das neueste Protokoll-Backup mit der nicht unterbrochenen Sequenz von Archivprotokollen nach dem Daten-Backup, das zum Klonen ausgewählt wurde, mounten. Die geklonte Datenbank wird wiederhergestellt, bis die fehlende oder beschädigte Protokolldatei vorliegt.
Datum und Uhrzeit	SnapCenter stellt die Datenbank bis zu einem festgelegten Datum und einer bestimmten Uhrzeit wieder her. Das akzeptierte Format lautet mm/TT/JJJJ hh:mm:ss Die Zeit kann im 24-Stunden-Format angegeben werden.

Feldname	Beschreibung
Bis SCN (Systemänderungsnummer)	SnapCenter stellt die Datenbank bis zu einer angegebenen Systemänderungsnummer (SCN) wieder her.
Geben Sie externe Archivprotokolle an	Wenn die Datenbank im ARCHIVELOG-Modus ausgeführt wird, identifiziert und montiert SnapCenter die optimale Anzahl von Protokoll-Backups basierend auf dem angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Zeit. Sie können auch den externen Speicherort für das Archivprotokoll angeben. SnapCenter identifiziert und Mounten die Backup-Protokolle nicht automatisch, wenn Sie bis zum Abbrechen ausgewählt haben.
Neue DBID erstellen	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 im externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.
Erstellen Sie eine tempfile für temporäre Tablespaces	Aktivieren Sie das Kontrollkästchen, wenn Sie eine tempfile für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten. Wenn das Kontrollkästchen nicht aktiviert ist, wird der Datenbankklon ohne die tempfile erstellt.
Geben Sie beim Erstellen eines Klons sql-Einträge ein, die angewendet werden sollen	Fügen Sie die sql-Einträge hinzu, die Sie beim Erstellen des Klons anwenden möchten.

Feldname	Beschreibung
Geben Sie Skripte ein, die nach dem Klonvorgang ausgeführt werden sollen	Geben Sie den Pfad und die Argumente des Postskripts an, die Sie nach dem Klonvorgang ausführen möchten. Das Postscript sollte entweder in */var/opt/snapcenter/spl/scripts* oder in einem Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird. Falls der Klonvorgang fehlschlägt, werden Postskripte nicht ausgeführt und Bereinigungstätigkeiten werden direkt ausgelöst.

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

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

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

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

    Während des Recovery im Rahmen des Klonens wird der Klon mit einer Warnung erstellt, auch wenn das Recovery fehlschlägt. Sie können für diesen Klon ein manuelles Recovery durchführen, um die Klondatenbank konsistent zu machen.

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

Ergebnis

Nach dem Klonen der Datenbank können Sie die Seite „Ressourcen“ aktualisieren, um die geklonte Datenbank als eine der für Backups verfügbaren Ressourcen aufzulisten. Die geklonte Datenbank kann mithilfe des Standard-Backup-Workflows wie jede andere Datenbank gesichert oder in eine Ressourcengruppe (entweder neu erstellt oder bereits vorhanden) aufgenommen werden. Die geklonte Datenbank kann weiter geklont werden (Klon von Klonen).

Nach dem Klonen sollten Sie die geklonte Datenbank niemals umbenennen.

Falls Sie das Recovery während des Klonens nicht durchgeführt haben, kann das Backup der geklonten Datenbank fehlschlagen, da ein unsachgemäßes Recovery erforderlich ist und Sie möglicherweise manuelles Recovery durchführen müssen. Das Protokoll-Backup kann auch fehlschlagen, wenn der Standardspeicherort, der für Archivprotokolle erfasst wurde, auf einem Storage anderer Anbieter liegt oder wenn das Storage-System nicht mit SnapCenter konfiguriert ist.

In AIX Setup können Sie den Befehl lkdev zum Sperren und den Befehl rendev verwenden, um die Festplatten umzubenennen, auf denen sich die geklonte Datenbank residierte.

Das Sperren oder Umbenennen von Geräten hat keine Auswirkungen auf den Löschvorgang. Bei AIX LVM-Layouts, die auf SAN-Geräten aufgebaut sind, werden die Umbenennung von Geräten für die geklonten SAN-Geräte nicht unterstützt.

Weitere Informationen

- "Die Wiederherstellung oder das Klonen schlägt mit der ORA-00308-Fehlermeldung fehl"
- "Fehler beim Wiederherstellen einer geklonten Datenbank"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Klonen einer sofort anschließbaren Datenbank

Sie können eine steckbare Datenbank (PDB) auf einem anderen oder demselben Ziel-CDB auf demselben Host oder einem anderen Host klonen. Sie können die geklonte PDB auch auf einem gewünschten SCN oder Datum und Uhrzeit wiederherstellen.

Bevor Sie beginnen

Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript 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 die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank des Typs Single Instance (mandantenfähig) aus der Detailansicht der Datenbank oder in der Detailansicht der Ressourcengruppen aus.

   Die Seite der Datenbanktopologie wird angezeigt.

4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (sekundär) aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   a. Wählen Sie **PDB Clone**.
   b. Geben Sie die PDB an, die Sie klonen möchten.

Sie können jeweils nur eine PDB klonen.

c. Geben Sie den Namen der Klon-PDB an.

7. Führen Sie auf der Seite Speicherorte die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonhost	Standardmäßig wird der Quell-Datenbank-Host befüllt. Wenn Sie den Klon auf einem anderen Host erstellen möchten, wählen Sie den Host aus, der dieselbe Version von Oracle und dasselbe Betriebssystem wie der des Quelldatenbankhosts hat.
Ziel-CDB	Wählen Sie die CDB aus, in die die geklonte PDB einbezogen werden soll. Sie sollten sicherstellen, dass die Ziel-CDB ausgeführt wird.
Datenbankstatus	Aktivieren Sie das Kontrollkästchen **Öffnen Sie die geklonte PDB im LESE-SCHREIBMODUS**, wenn Sie die PDB im LESE-SCHREIB-Modus öffnen möchten.
Datendateiorte	Standardmäßig wird der Speicherort der Datendatei gefüllt. Die standardmäßige Namenskonvention von SnapCenter für SAN- oder NFS-Dateisysteme ist FileSystemNamesourceDatabase_SCJOBID. Die standardmäßige SnapCenter-Namenskonvention für ASM-Festplattengruppen ist SC_HASHCODEofDISKGROUP_SCJOBID. Die HASHCODEofDISKGROUP ist eine automatisch generierte Nummer (2 bis 10 Ziffern), die für jede ASM-Laufwerksgruppe eindeutig ist. Wenn Sie den Namen der ASM-Laufwerksgruppe anpassen, stellen Sie sicher, dass die Namenslänge die von Oracle unterstützte maximale Länge erfüllt. Wenn Sie einen anderen Pfad angeben möchten, müssen Sie die Mount-Punkte für Datendatei oder die Namen der ASM-Festplattengruppen für die Klondatenbank eingeben.

Die Oracle-Startseite, der Benutzername und die Gruppendetails werden automatisch aus der Quelldatenbank ausgefüllt. 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 für das Prescript ein, das Sie vor dem Klonvorgang ausführen möchten.

      Sie sollten das Prescript entweder in /var/opt/snapcenter/spl/scripts oder in einem Ordner in diesem Pfad speichern. Standardmäßig wird der Pfad /var/opt/snapcenter/spl/scripts ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird.

   Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie das Skript und das Postscript ausführen. "Weitere Informationen ."

   a. Ändern Sie im Abschnitt Parametereinstellungen der Zusatzdatenbank CDB Clone die Werte vorbefüllter Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.

9. Klicken Sie auf **Zurücksetzen**, um die Standardeinstellungen für die Datenbankparameter anzuzeigen.
10. Auf der PostOps-Seite ist **bis Abbrechen** standardmäßig ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

    Die Option **bis Abbrechen** wird nicht ausgewählt, wenn SnapCenter die entsprechenden Log-Backups nicht findet. Sie können den externen Archiv-Log-Speicherort angeben, wenn die Protokollsicherung in **externen Archiv-Log-Speicherorten angeben** nicht verfügbar ist. Sie können mehrere Protokollpositionen 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	SnapCenter führt eine Recovery durch, indem das neueste Protokoll-Backup mit der nicht unterbrochenen Sequenz von Archivprotokollen nach dem Daten-Backup, das zum Klonen ausgewählt wurde, mounten. Das Protokoll und das Daten-Backup sollten sich auf dem Primärspeicher befinden, um den Klon im Primärspeicher durchzuführen und Protokoll- und Daten-Backups auf dem Sekundärspeicher zu erstellen, um den Klon im Sekundärspeicher durchzuführen. Die geklonte Datenbank wird wiederhergestellt, bis die fehlende oder beschädigte Protokolldatei vorliegt.

Feldname	Beschreibung
Datum und Uhrzeit	SnapCenter stellt die Datenbank bis zu einem festgelegten Datum und einer bestimmten Uhrzeit wieder her. Die Zeit kann im 24-Stunden-Format angegeben werden.
Bis SCN (Systemänderungsnummer)	SnapCenter stellt die Datenbank bis zu einer angegebenen Systemänderungsnummer (SCN) wieder her.
Geben Sie externe Archivprotokolle an	Geben Sie den Speicherort des externen Archivprotokolls an.
Neue DBID erstellen	Standardmäßig ist das Kontrollkästchen Neue DBID* erstellen nicht für die Zusatzklondatenbank ausgewählt. Aktivieren Sie das Kontrollkästchen, wenn Sie eine eindeutige Nummer (DBID) für die zusätzliche geklonte Datenbank generieren möchten, die sie von der Quelldatenbank unterscheidet.
Erstellen Sie eine tempfile für temporäre Tablespaces	Aktivieren Sie das Kontrollkästchen, wenn Sie eine tempfile für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten. Wenn das Kontrollkästchen nicht aktiviert ist, wird der Datenbankklon ohne die tempfile erstellt.
Geben Sie beim Erstellen eines Klons sql-Einträge ein, die angewendet werden sollen	Fügen Sie die sql-Einträge hinzu, die Sie beim Erstellen des Klons anwenden möchten.

Feldname	Beschreibung
Geben Sie Skripte ein, die nach dem Klonvorgang ausgeführt werden sollen	Geben Sie den Pfad und die Argumente des Postskripts an, die Sie nach dem Klonvorgang ausführen möchten. Das Postscript sollte entweder in */var/opt/snapcenter/spl/scripts* oder in einem Ordner in diesem Pfad gespeichert werden. Standardmäßig ist der Pfad */var/opt/snapcenter/spl/scripts* ausgefüllt. Wenn Sie das Skript in einem beliebigen Ordner innerhalb dieses Pfads platziert haben, müssen Sie den vollständigen Pfad zum Ordner angeben, in dem das Skript abgelegt wird. Falls der Klonvorgang fehlschlägt, werden Postskripte nicht ausgeführt und Bereinigungstätigkeiten werden direkt ausgelöst.

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

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

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

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

Nach Ihrer Beendigung

Wenn Sie eine Sicherung der geklonten PDB erstellen möchten, sollten Sie die Ziel-CDB dort sichern, wo die PDB geklont wird, da eine Sicherung nur der geklonten PDB nicht möglich ist. Sie sollten eine sekundäre Beziehung für das Ziel-CDB erstellen, wenn Sie die Sicherung mit einer sekundären Beziehung erstellen möchten.

In einem RAC-Setup ist der Speicher für geklonte PDB nur mit dem Knoten verbunden, auf dem der PDB-Klon ausgeführt wurde. Die PDBs auf den anderen Knoten des RAC befinden sich im MOUNT-Status. Wenn Sie möchten, dass die geklonte PDB von den anderen Nodes aus zugänglich ist, sollten Sie den Storage manuell den anderen Nodes zuweisen.

Weitere Informationen

- "Die Wiederherstellung oder das Klonen schlägt mit der ORA-00308-Fehlermeldung fehl"
- "Anpassbare Parameter für Backup-, Wiederherstellungs- und Klonvorgänge auf AIX-Systemen"

Backups der Oracle Datenbank mit UNIX Befehlen klonen

Der Klon-Workflow umfasst die Planung, die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

Sie sollten die folgenden Befehle ausführen, um die Oracle Database Clone Specification File zu erstellen und den Klonvorgang zu starten.

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

Schritte

1. Erstellen Sie eine Oracle-Datenbankklonspezifikation aus einem angegebenen Backup: *New-SmOracleCloneSpecification*

   Wenn die sekundäre Datenschutzrichtlinie ein einheitliches Mirror-Vault ist, geben Sie nur -IncludeSecond Details an. Sie müssen nicht -SecondaryStorageType angeben.

   Mit diesem Befehl wird automatisch eine Oracle-Datenbankklonspezifikationsdatei für die angegebene Quelldatenbank und ihr Backup erstellt. Außerdem müssen Sie eine Klon-Datenbank-SID angeben, damit die erstellte Spezifikationsdatei die automatisch generierten Werte für die von Ihnen erstellte Klondatenbank enthält.

   Die Klon-Spezifikations-Datei wird unter */var/opt/snapcenter/sco/Clone_specs* erstellt.

2. Initiieren einer Klonoperation aus einer Clone Resource Group oder einem vorhandenen Backup: *New-SmClone*

   Dieser Befehl initiiert einen Klonvorgang. Für den Klonvorgang müssen Sie außerdem einen Pfad für die Oracle-Klonspezifikation angeben. Zudem können Sie die Recovery-Optionen festlegen, auf denen der Klonvorgang ausgeführt werden soll, sowie Vorskripte, Postskripte und andere Details.

   Standardmäßig wird die Zieldatei des Archivprotokolls für die Klondatenbank automatisch mit einer Zieldatei von _ € ORACLE_HOME/CLONE_SIDs_ gefüllt.

Oracle Database klonen

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

Über diese Aufgabe

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

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

Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

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

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie im "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Datenbank** aus.
3. Wählen Sie die geklonte Ressource aus (z. B. die Datenbank oder die LUN), und klicken Sie dann auf  .
4. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Klonabteilvorgang reagiert nicht mehr, wenn der SMCore-Service neu gestartet wird und die Datenbanken, auf denen der Klonabteilvorgang ausgeführt wurde, als Klone auf der Seite Ressourcen aufgeführt werden. Sie sollten das Cmdlet *Stop-SmJob* ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragezeit benötigen, um zu prüfen, ob der Klon aufgeteilt ist oder nicht, können Sie den Wert von CloneSplitStatusCheckPollTime in der Datei SMCoreServiceHost.exe.config ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Klonabteilvorgangs abgefragt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

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

Der Startvorgang für die Klontrennung schlägt fehl, wenn derzeit eine Sicherung, Wiederherstellung oder eine andere Klonverteilung durchgeführt wird. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Split-Klon einer steckbaren Datenbank

Sie können eine geklonte Plug-in-Datenbank (PDB) mit SnapCenter teilen.

Über diese Aufgabe

Wenn Sie eine Sicherung der Ziel-CDB erstellt haben, in der die PDB geklont wird, wird die geklonte PDB bei der Aufteilung des PDB-Klons auch aus allen Backups der Ziel-CDB entfernt, die die geklonte PDB enthalten.

Die PDB-Klone werden in der Ansicht „Inventar“ oder „Ressourcen“ nicht 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 Quellcontainer-Datenbank (CDB) aus der Ressourcen- oder Ressourcengruppenansicht aus.
3. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
4. Wählen Sie den PDB-Klon (targetCDB:PDBClone) aus und klicken Sie dann auf  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Überwachen Sie die Klonvorgänge von Oracle Datenbanken

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

Über diese Aufgabe

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

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

Schritte

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

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

Aktualisieren Sie einen Klon

Sie können den Klon aktualisieren, indem Sie den Befehl *Refresh-SmClone* ausführen. Mit diesem Befehl wird ein Backup der Datenbank erstellt, der vorhandene Klon gelöscht und ein Klon mit demselben Namen erstellt.

Ein PDB-Klon kann nicht aktualisiert werden.

Was Sie brauchen

- Erstellen Sie ein komplettes Online-Backup oder eine Offline Daten-Backup-Richtlinie, ohne dass geplante Backups aktiviert sind.
- Konfigurieren Sie die E-Mail-Benachrichtigung in der Richtlinie nur für Backup-Fehler.
- Definieren Sie die Aufbewahrungszahl für die On-Demand-Backups entsprechend, um sicherzustellen, dass keine unerwünschten Backups vorhanden sind.
- Stellen Sie sicher, dass nur ein vollständiges Online-Backup oder eine Richtlinie für Offline-Daten-Backups der Ressourcengruppe zugeordnet ist, die für den Klon-Aktualisierungsvorgang ermittelt wird.
- Erstellen Sie eine Ressourcengruppe mit nur einer Datenbank.
- Wenn ein Cron-Job für den Befehl „Clone Refresh“ erstellt wird, stellen Sie sicher, dass sich die SnapCenter-Zeitpläne und cron-Zeitpläne nicht mit der Datenbankressourcengruppe überschneiden.

  Stellen Sie für einen Cron-Job, der für den Befehl „Clone refresh“ erstellt wurde, sicher, dass Sie Open-SmConnection nach allen 24 Stunden ausführen.

- Stellen Sie sicher, dass die Klon-SID für einen Host eindeutig ist.

  Wenn mehrere Aktualisierungsklonvorgänge dieselbe Klon-Spezifikationsdatei verwenden oder die Klon-Spezifikationsdatei mit derselben Clone-SID verwenden, wird der vorhandene Klon mit der SID auf dem Host gelöscht und dann der Klon erstellt.

- Stellen Sie sicher, dass die Backup-Richtlinie mit sekundärem Schutz aktiviert ist und dass die Klon-Spezifikations-Datei mit „`-IncludeSecondaryDetails`“ erstellt wird, um die Klone mit sekundären Backups zu erstellen.
  - Wenn die Spezifikationsdatei für den primären Klon angegeben ist, die Richtlinie jedoch die Option für das sekundäre Update ausgewählt hat, wird das Backup erstellt und das Update wird auf den sekundären Server übertragen. Der Klon wird jedoch aus dem primären Backup erstellt.
  - Wenn die Spezifikations-Datei für den primären Klon angegeben ist und für die Richtlinie keine Option für das sekundäre Update ausgewählt ist, wird das Backup auf dem primären erstellt und der Klon aus dem primären erstellt.

Schritte

1. Initiieren Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer: *Open-SmConnection*
2. Erstellen Sie eine Oracle-Datenbankklonspezifikation aus einem angegebenen Backup: *New-SmOracleCloneSpecification*

Wenn die sekundäre Datenschutzrichtlinie ein einheitliches Mirror-Vault ist, geben Sie nur -IncludeSecond Details an. Sie müssen nicht -SecondaryStorageType angeben.

Mit diesem Befehl wird automatisch eine Oracle-Datenbankklonspezifikationsdatei für die angegebene Quelldatenbank und ihr Backup erstellt. Außerdem müssen Sie eine Klon-Datenbank-SID angeben, damit die erstellte Spezifikationsdatei die automatisch generierten Werte für die von Ihnen erstellte Klondatenbank enthält.

Die Klon-Spezifikations-Datei wird unter */var/opt/snapcenter/sco/Clone_specs* erstellt.

3. Führen Sie *Refresh-SmClone* aus.

   Falls der Vorgang mit der Fehlermeldung „PL-SCO-20032: CanExecute fehlgeschlagen mit Fehler: PL-SCO-30031: Redo Log file +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists“, geben Sie einen höheren Wert für die Fehlermeldungen *-WaitToTriggerClone* an.

   Ausführliche Informationen zu UNIX-Befehlen finden Sie im "SnapCenter Software Command Reference Guide".

Löschen des Klons einer steckbaren Datenbank

Sie können den Klon einer steckbaren Datenbank (PDB) löschen, wenn Sie nicht mehr benötigen.

Wenn Sie eine Sicherung der Ziel-CDB erstellt haben, wo die PDB geklont wird, wird beim Löschen des PDB-Klons auch die geklonte PDB aus der Sicherung der Ziel-CDB entfernt.

Die PDB-Klone werden in der Ansicht „Inventar“ oder „Ressourcen“ nicht 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 Quellcontainer-Datenbank (CDB) aus der Ressourcen- oder Ressourcengruppenansicht aus.
3. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
4. Wählen Sie den PDB-Klon (targetCDB:PDBClone) aus und klicken Sie dann auf .
5. Klicken Sie auf **OK**.

Management von Applikations-Volumes

Was sind Applikations-Volumes

Anwendungsvolumes sind der Speicher, in dem Informationen wie Konfigurations-, Installer- und andere nicht-Datendateien im Zusammenhang mit der Oracle-Datenbank gespeichert werden.

Das SnapCenter Plug-in für Oracle Database ermöglicht Ihnen die Erstellung eines konsistenten Backups von

Applikations-Volumes (nicht-Datenvolumen) zusammen mit den Oracle Datenbanken.

Das Plug-in automatisiert das Backup und das Klonen von Applikations-Volumes.

- Schützen Sie Anwendungs-Volumes zusammen mit Oracle Database Volumes in einer einzigen Ressourcengruppe.
- Erstellen Sie Backups von Applikations-Volumes.
- Erstellen Sie Backups von Oracle Datenbanken zusammen mit Applikations-Volumes.
- Erstellen Sie bis zu zeitpunktbezogene Klone von Datenbanken und Applikations-Volumes.
- Planen von Backup-Vorgängen
- Monitoring aller Vorgänge
- Anzeigen von Berichten zu Backup- und Klonvorgängen

Hinzufügen von Applikations-Volumes

SnapCenter unterstützt das Backup und Klonen von Applikations-Volumes einer Oracle Datenbank. Sie sollten die Anwendungsvolumes manuell hinzufügen. Die automatische Erkennung von Applikations-Volumes wird nicht unterstützt.

Applikations-Volumes unterstützen nur direkte NFS- und iSCSI-Verbindungen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Datenbank-Plug-in aus der Liste aus.
2. Klicken Sie Auf **Anwendungsvolumen Hinzufügen**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   - 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 Speicherabdruck den Namen des Speichersystems ein, wählen Sie ein oder mehrere Volumes aus und geben Sie die zugehörigen LUNs oder qtrees an.

   Sie können mehrere Storage-Systeme hinzufügen.

5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
6. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Anwendungsvolumen** aus, um alle Anwendungsvolumes anzuzeigen, die Sie hinzugefügt haben.

Anwendungsvolumen ändern

Wenn keine Backups erstellt werden, können Sie alle Werte ändern, die Sie beim Hinzufügen des Anwendungs-Volumes angegeben haben. Wenn das Backup erstellt wird, können Sie nur die Details des Speichersystems ändern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Datenbank-Plug-in aus der Liste aus.

2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Anwendungsvolumen** aus.
3. Klicken Sie auf  , um die Werte zu ändern.

Anwendungsvolumen löschen

Wenn Sie ein Applikations-Volume löschen, werden im Falle von Backups, die mit dem Applikations-Volume verbunden sind, das Applikations-Volume in den Wartungsmodus versetzt, ohne dass neue Backups erstellt werden und keine früheren Backups erhalten werden. Wenn keine Backups zugeordnet sind, werden alle Metadaten gelöscht.

Falls erforderlich, können Sie mit SnapCenter den Löschvorgang rückgängig machen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Datenbank-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Anwendungsvolumen** aus.
3. Klicken Sie auf  , um die Werte zu ändern.

Backup-Anwendungsvolumes

Backup des Anwendungsvolumes

Wenn das Anwendungs-Volume nicht Teil einer Ressourcengruppe ist, können Sie das Anwendungs-Volume von der Seite Ressourcen sichern.

Über diese Aufgabe

Standardmäßig werden Backups von Konsistenzgruppen (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 Datenbank-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** 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 klicken  , um den Filterbereich zu schließen.
4. Wählen Sie das Anwendungsvolumen aus, das Sie sichern möchten.

   Die Seite Volume-Protect der Anwendung wird angezeigt.
5. Führen Sie auf der Seite „Ressource“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll. Beispiel: Custtext__Policy_hostname oder Resource_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.
Ausschließen von Zielen für Archivprotokolle von der Sicherung	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 Dropdown-Liste aus.

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

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

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

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

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den Backup-Vorgang anhängen möchten, der an der Ressource durchgeführt wird, und dann wählen Sie **Job-Bericht anhängen**.

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

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

   Die Topologieseite des Anwendungs-Volumes wird angezeigt.

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

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

b. Klicken Sie Auf **Backup**.

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

Sichern Sie die Ressourcengruppe Anwendungsvolumes

Sie können ein Backup der Ressourcengruppe erstellen, die nur Applikations-Volumes oder eine Mischung aus Applikations-Volumes und Datenbank enthält. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Wenn die Ressourcengruppe mehrere Anwendungs-Volumes hat, sollten alle Anwendungs-Volumes entweder über SnapMirror oder SnapVault-Replizierungsrichtlinie verfügen.

Über diese Aufgabe

Standardmäßig werden Backups von Konsistenzgruppen (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 Datenbank-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf , klicken und dann das Tag auswählen. Sie können dann 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

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

> Der Verifizierungsvorgang wird nur für die Datenbanken und nicht für die Applikations-Volumes durchgeführt.

Backup von Klon-Applikations-Volumes

Sie können SnapCenter zum Klonen der Backups des Applikations-Volumes verwenden.

Bevor Sie beginnen

Wenn Sie das Plug-in als nicht-root-Benutzer installiert haben, sollten Sie die Ausführungsberechtigungen manuell den Verzeichnissen Prescript und Postscript zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Datenbank-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Anwendungsvolumen** aus.
3. Wählen Sie das Anwendungs-Volume entweder in der Detailansicht des Anwendungs-Volumes oder in der Detailansicht Ressourcengruppen aus.

   Die Topologieseite des Anwendungs-Volumes wird angezeigt.
4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (sekundär) aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
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 Skripts die Namen der vor dem Klonen auszuführenden Skripte, Befehle zum Mounten eines Dateisystems und Namen der nach dem Klonen auszuführenden Skripte an.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

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

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Einen Applikations-Volume-Klon aufteilen

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Datenbank-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Anwendungsvolumen** aus.

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

Löschen eines Applikations-Volume-Klons

Klone können gelöscht werden, wenn Sie sie nicht mehr benötigen. Klone, die sich als Quelle für andere Klone fungieren, können nicht gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Oracle Datenbank-Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Anwendungsvolumen** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Ressource“ oder „Topologie der Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
5. Wählen Sie den Klon aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Klonen löschen die folgenden Aktionen durch:
   a. Geben Sie im Feld **Pre Clone delete** die Namen der zu ausführenden Skripte ein, bevor Sie den Klon löschen.
   b. Geben Sie im Feld **Unmount** die Befehle ein, um die Bereitstellung des Klons zu deaktivieren, bevor Sie den Klon löschen.
7. Klicken Sie auf **OK**.

Sichern Sie Windows Filesysteme

SnapCenter Plug-in für Microsoft Windows-Konzepte

SnapCenter Plug-in für Microsoft Windows – Übersicht

Das SnapCenter Plug-in für Microsoft Windows ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das applikationsgerechte Datensicherungsmanagement von Microsoft Filesystem-Ressourcen ermöglicht. Darüber hinaus bietet sie Storage-Bereitstellung, Snapshot Konsistenz und Speicherplatzrückgewinnung für Windows Filesysteme. Das Plug-in für Windows automatisiert Backup, Wiederherstellung und Klonvorgänge in File-Systemen in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für Windows installiert ist, können Sie SnapCenter mit NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Zusammen mit der NetApp SnapVault Technologie können Sie eine Disk-to-Disk-Backup-Replizierung für Archivierung oder Standards durchführen.

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 mithilfe von SnapCenter Windows File-Systeme sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

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

Das Plug-in für Windows unterstützt keine Backups und Restores von Filesystemen auf SMB-Freigaben.

SnapCenter Plug-in für Windows Funktionen

Das Plug-in für Windows ist in NetApp Snapshot Technologie auf dem Storage-System integriert. Um mit dem Plug-in für Windows zu arbeiten, verwenden Sie die SnapCenter-Schnittstelle.

Das Plug-in für Windows umfasst folgende Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche powered by SnapCenter**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die Schnittstelle von SnapCenter ermöglicht die vollständige konsistente Backup- und Restore-

Prozesse über Plug-ins hinweg, die zentrale Berichterstellung, die auf einen Blick basierende Dashboard-Ansichten verwenden, die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) einrichten und Jobs in allen Plug-ins überwachen. SnapCenter bietet außerdem eine zentralisierte Planung und ein Richtlinienmanagement zur Unterstützung von Backup- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

  Sie können routinemäßige File-System-Backups planen, die Backup-Aufbewahrung richtlinienbasiert konfigurieren und Restore-Vorgänge einrichten. Zudem lässt sich die File-System-Umgebung proaktiv überwachen, indem SnapCenter so konfiguriert wird, dass E-Mail-Warnmeldungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshots**

  Das Plug-in für Windows verwendet NetApp Snapshot Technologie. So können Sie File-Systeme in Sekundenschnelle sichern und schnell wiederherstellen, ohne das Host offline zu schalten. Snapshots belegen nur minimalen Speicherplatz.

Zusätzlich zu diesen wichtigen Funktionen bietet das Plug-in für Windows folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation
- Erstellung platzsparender Kopien von Produktionsdateisystemen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

  Weitere Informationen zur FlexClone Lizenzierung finden Sie unter "SnapCenter-Lizenzen".

- Die Möglichkeit, mehrere Backups gleichzeitig über mehrere Server hinweg auszuführen
- PowerShell cmdlets zur Skripte von Backup-, Wiederherstellungs- und Klonvorgängen
- Unterstützung von Backups von Dateisystemen und Virtual Machine Disks (VMDKs)
- Unterstützung physischer und virtualisierter Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK über NFS und VMFS und Virtual FC
- Unterstützung für Non-Volatile Memory Express (NVMe) unter Windows Server 2022
  - Backup-, Restore-, Klon- und Verifizierungsworkflows auf VMDK-Layout, das auf NVMe over TCP/IP erstellt wurde.
  - Unterstützt NVMe-Firmware-Version 1.3 ab ESX 8.0 Update 2 und erfordert Virtual Hardware-Version 21.
  - Windows Server Failover Clustering (WSFC) wird nicht für Applikationen über VMDK auf NVMe over TCP/IP unterstützt.
- Unterstützung von SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Business Services auch bei einem vollständigen Standortausfall weiterlaufen können und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.

Wie SnapCenter Windows File-Systeme sichert

SnapCenter nutzt die Snapshot Technologie, um Windows File-System-Ressourcen zu sichern, die sich auf LUNs, CSVs (Cluster Shared Volumes), RDM (Raw Device

Mapping)-Volumes, ALM (asymmetrische LUN-Zuordnung) in Windows Clustern und VMDKs auf Basis von VMFS/NFS (VMware Virtual Machine File System über NFS) befinden.

SnapCenter erstellt Backups durch Erstellen von Snapshots der Dateisysteme. Gebündelte 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 Vergleich zu individuellen Snapshots jedes Filesystems.

Wenn SnapCenter einen Snapshot erstellt, wird im Snapshot das gesamte Storage-System-Volume erfasst. Die Sicherung ist jedoch nur für den Host-Server gültig, für den das Backup 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 Storage-Typen

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines. Sie müssen überprüfen, ob Ihr Speichertyp unterstützt wird, bevor Sie das Paket für Ihren Host installieren.

SnapCenter Provisioning und Datensicherung werden unter Windows Server unterstützt. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische SnapCenter Benutzeroberfläche (GUI) oder PowerShell Commandlets	
Physischer Server	ISCSI-verbundene LUNs	SnapCenter GUI oder PowerShell Commandlets	
Physischer Server	SMB3 (CIFS) Shares auf einer Storage Virtual Machine (SVM)	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung.
VMware VM	RDM-LUNs, die über einen FC- oder iSCSI-HBA verbunden sind	PowerShell Commandlets	
VMware VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
VMware VM	Virtual Machine File Systems (VMFS) oder NFS-Datastores	VMware vSphere	
VMware VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung.
VMware VM	VVol Datastores auf NFS und SAN	ONTAP Tools für VMware vSphere	
Hyper-V VM	Virtuelle FC-LUNs (VFC), die über einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Sie müssen Hyper-V Manager verwenden, um virtuelle FC (VFC) LUNs bereitzustellen, die über einen virtuellen Fibre Channel Switch verbunden sind.  Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.
Hyper-V VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Minimale ONTAP-Berechtigungen für Windows Plug-in erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun

- lun erstellen
- lun löschen
- lun Initiatorgruppe hinzufügen
- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen

    - Show-Disk-Nutzung für Volume-Dateien
    - Volume ist offline
    - Das Volume ist online
    - Volume-Änderung
    - Erstellen von Volume-qtree
    - Volume qtree löschen
    - Änderung des Volume-qtree
    - Volume-qtree anzeigen
    - Volume-Einschränkung
    - Volumen anzeigen
    - Erstellen von Volume-Snapshots
    - Volume Snapshot löschen
    - Ändern des Volume-Snapshots
    - Umbenennung von Volume-Snapshots
    - Wiederherstellung von Volume Snapshots
    - Restore-Datei für Volume Snapshots
    - Volume-Snapshot werden angezeigt
    - Volume-Aufhängung nicht verfügbar
    - cifs von vserver
    - erstellung von cifs-Freigaben von vserver
    - cifs-Freigabe von vserver: Löschen
    - vserver cifs shadowcopy anzeigen
    - cifs-Freigabe von vserver wird angezeigt
    - vserver cifs zeigen
    - vserver Exportrichtlinie
    - Erstellung von vserver Exportrichtlinien
    - vserver: Löschen der Exportrichtlinie
    - Erstellung von vserver Export-Policy-Regel
    - vserver: Export-Policy-Regel anzeigen
    - vserver Export-Policy wird angezeigt
    - vserver iscsi
    - vserver iscsi-Verbindung wird angezeigt
    - vserver zeigen
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle
    - Netzwerkschnittstelle wird angezeigt
    - vserver

Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

> Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

> SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Definieren einer Backup-Strategie für Windows File-Systeme

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backups erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre File-Systeme erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Backup-Pläne für Windows File-Systeme

Die Sicherungshäufigkeit wird in den Richtlinien angegeben. Ein Backup-Zeitplan wird in der Konfiguration der Ressourcengruppe angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können beispielsweise die Sicherungshäufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren oder Sie können **Keine** angeben, wodurch die Richtlinie eine reine On-Demand-Richtlinie darstellt. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Backups konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Windows File-Systeme benötigten Backups

Faktoren, die die Anzahl der erforderlichen Backups bestimmen, umfassen die Größe des Windows-Dateisystems, die Anzahl der verwendeten Volumes, die Änderungsrate des Dateisystems und die Service Level Agreement (SLA).

Backup Namenskonvention für Windows File-Systeme

Für Windows-Dateisystem-Backups wird die standardmäßige Snapshot-Namenskonvention verwendet. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Der Snapshot verwendet die folgende Standard-Namenskonvention:
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 Bedeutungen:

- `dts1` Ist der Name der Ressourcengruppe.
- `mach1x88` Ist der Hostname.
- `03-12-2016_23.17.26` Ist das Datum und der Zeitstempel.

Beim Erstellen eines Backups können Sie auch ein beschreibende Tag hinzufügen, um das Backup zu

identifizieren. Wenn Sie hingegen eine angepasste Backup-Namenskonvention verwenden möchten, müssen Sie das Backup umbenennen, nachdem der Backup-Vorgang abgeschlossen ist.

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Quellen und Ziele von Klonen für Windows Filesysteme

Sie können ein File-System-Backup vom primären oder sekundären Storage klonen. Sie können auch das Ziel wählen, das Ihre Anforderungen unterstützt: Entweder den ursprünglichen Backup-Standort oder ein anderes Ziel auf demselben Host oder auf einem anderen Host. Das Ziel muss sich auf demselben Volume befinden wie das Quellbackup des Klons.

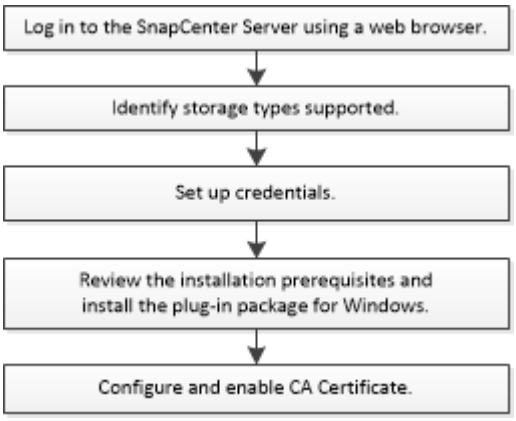
Klonziel	Beschreibung
Original, Quelle, Standort	Standardmäßig speichert SnapCenter den Klon am selben Standort und auf demselben Host wie das zu klonendes Backup.
Andere Position	Sie können den Klon an einem anderen Ort auf demselben Host oder auf einem anderen Host speichern. Der Host muss über eine konfigurierte Verbindung zur Storage Virtual Machine (SVM) verfügen.

Sie können den Klon nach Abschluss des Klonvorgangs umbenennen.

Installieren Sie das SnapCenter Plug-in für Microsoft Windows

Installationsworkflow des SnapCenter Plug-ins für Microsoft Windows

Sie müssen SnapCenter-Plug-in für Microsoft Windows installieren und einrichten, wenn Sie Windows-Dateien, die keine Datenbankdateien sind, schützen möchten.



Installationsanforderungen für das SnapCenter Plug-in für Microsoft Windows

Vor der Installation des Plug-ins für Windows sollten Sie sich über bestimmte Installationsanforderungen im Klaren sein.

Bevor Sie mit der Verwendung des Plug-ins für Windows beginnen, muss der SnapCenter-Administrator SnapCenter Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Um das Plug-in für Windows zu installieren, müssen Sie über die Administratorrechte von SnapCenter verfügen.

  Die SnapCenter-Administratorrolle muss über Administratorrechte verfügen.

- Sie müssen den SnapCenter-Server installiert und konfiguriert haben.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Sie müssen SnapMirror und SnapVault einrichten, wenn Sie eine Backup-Replizierung möchten.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Wenn Sie ein Windows-Cluster-Setup verwenden, sollten Sie auch die Windows-Remoteverwaltung (WinRM) installieren und konfigurieren.
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Richten Sie Ihre Anmeldedaten für das Plug-in für Windows ein

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins erstellen und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen auf Windows-Dateisystemen erhalten.

Was Sie brauchen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.
- Sie müssen die Anmeldedaten auf dem Remote-Host mit Administratorrechten, einschließlich Administratorrechten, einrichten.
- Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzer keine vollständigen Administratorberechtigungen hat, müssen Sie dem Benutzer mindestens die Gruppen- und Sicherungsrechte zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Gehen Sie auf der Seite Credential wie folgt vor:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die für die Authentifizierung verwendet werden. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld Benutzername lautet wie folgt: `UserName` Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.

5. Klicken Sie auf **OK**.

   Nachdem Sie die Einrichtung von Anmeldeinformationen abgeschlossen haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung von Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows

Sie können die Seite SnapCenter Add Host 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 ein 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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-

Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Der SnapCenter-Benutzer sollte der Rolle „`Anmelden als Dienst`“ des Windows-Servers hinzugefügt werden.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange in Betrieb ist.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2016 oder höher für Windows File System"

Über diese Aufgabe

- 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 installieren (WSFC, Oracle RAC oder Exchange DAG), sind sie auf allen Knoten des Clusters installiert.

- E-Series Storage

  Sie können das Plug-in für Windows nicht auf einem mit E-Series Storage verbundenen Windows-Host installieren.

> SnapCenter unterstützt das Hinzufügen desselben Hosts (Plug-in-Host) zu SnapCenter nicht, 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. Vergewissern Sie sich, dass **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ **Windows** aus. SnapCenter Server fügt den Host hinzu und installiert dann das Plug-in für Windows, falls es nicht bereits auf dem Host installiert ist.
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den vollständig qualifizierten Domänennamen (FQDN) einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Windows Server-Failover-Clustering (WSFC) Wenn Sie einen Host mit SnapCenter hinzufügen und dieser Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie den Anmeldeinformationsnamen aus, den Sie erstellt haben, oder erstellen Sie die neuen Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Details zu Anmeldeinformationen, einschließlich Benutzername, Domäne und Hosttyp, werden angezeigt, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen platzieren. Der Authentifizierungsmodus wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Bei neuen Implementierungen werden keine Plug-in-Pakete aufgeführt.

6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist C:\Programmdateien\NetApp\SnapCenter. 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.
Fügen Sie alle Hosts im Cluster hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Cluster-Nodes in einem WSFC hinzuzufügen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: *Domainname\AccountName€*. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird der Host

überprüft, ob er die Voraussetzungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version und -Standort werden mit den Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit Speicherplatz oder RAM zusammenhängt, können Sie die Datei Web.config in WebApp aktualisieren `C:\Program Files\NetApp\SnapCenter` , 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. Überwachen Sie den Installationsfortschritt.

Installieren Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Remote Hosts mithilfe von PowerShell cmdlets

Wenn Sie das SnapCenter-Plug-in für Microsoft Windows auf mehreren Hosts gleichzeitig installieren möchten, können Sie dies mit dem Cmdlet von PowerShell tun `Install-SmHostPackage` .

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie Plug-ins installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter Server-Host eine Sitzung mit dem `Open-SmConnection` Cmdlet und geben Sie dann Ihre Zugangsdaten ein.
3. Fügen Sie den eigenständigen Host oder das Cluster mit dem Cmdlet und den erforderlichen Parametern zu SnapCenter hinzu `Add-SmHost` .

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

4. Installieren Sie das Plug-in mit dem Cmdlet und den erforderlichen Parametern auf mehreren Hosts `Install-SmHostPackage` .

   Sie können die Option verwenden `-skipprecheck` , 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-Benutzeroberfläche installieren können. Sie können das SnapCenter-Plug-in für Microsoft Windows-Installationsprogramm unbeaufsichtigt, im Silent-Modus, über die Windows-Befehlszeile ausführen.

Bevor Sie beginnen

- Sie müssen Microsoft .Net 4.7.2 oder höher installiert haben.
- Sie müssen PowerShell 7.4.2 oder höher installiert haben.
- Sie müssen die Windows-Nachrichtenwarteschlange aktiviert 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.

   Beispielsweise lautet der Standardinstallationspfad C:\ProgramData\NetApp\SnapCenter\Package Repository.

   Auf diesen Pfad kann von dem Host 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 zum Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben.
4. Geben Sie den folgenden Befehl ein und ersetzen Sie 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`
   ```

   Alle Parameter, die während der Installation von Plug-in für Windows übergeben wurden, sind Groß- und Kleinschreibung.

   Geben Sie die Werte für die folgenden Variablen ein:

Variabel	Wert
/Debuglog“<Debug_Log_Path>	Geben Sie den Namen und den Speicherort der Protokolldatei für das Installationsprogramm der Suite an, wie im folgenden Beispiel: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Geben Sie den Port an, auf dem SnapCenter mit SMCore kommuniziert.

Variabel	Wert
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis für das Host-Plug-in-Paket an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter-Plug-in für das Web-Service-Konto von Microsoft Windows an.
BI_SERVICEPWD	Geben Sie das Passwort für das SnapCenter-Plug-in für das Microsoft Windows-Webservice-Konto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host implementiert werden soll.

Der Parameter *debuglog* enthält den Pfad der Protokolldatei für SnapCenter. Das Schreiben in diese Protokolldatei ist die bevorzugte Methode, um Informationen zur Fehlerbehebung zu erhalten, da die Datei die Ergebnisse von Prüfungen enthält, die die Installation für Plug-in-Voraussetzungen ausführt.

Weitere Informationen zur Fehlerbehebung finden Sie bei Bedarf in der Protokolldatei für das Paket SnapCenter für Windows. Die Protokolldateien für das Paket werden (älteste zuerst) im Ordner *%Temp%* aufgeführt, z. B. *C:\temp*\.

Die Installation des Plug-ins für Windows registriert das Plug-in auf dem Host und nicht auf dem SnapCenter-Server. Sie können das Plug-in auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Nach dem Hinzufügen des Hosts wird das Plug-in automatisch erkannt.

Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets

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

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden,

gehen Sie wie folgt vor:

a. Klicken Sie Auf **Filter**.
b. Optional: Geben Sie das Start- und Enddatum an.
c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
e. Klicken Sie Auf **Anwenden**.

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige**

Stammzertifizierungsbehörden > **Zertifikate**.

5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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"
   ```

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.

- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

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

Konfigurieren Sie die CRL-Datei

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

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

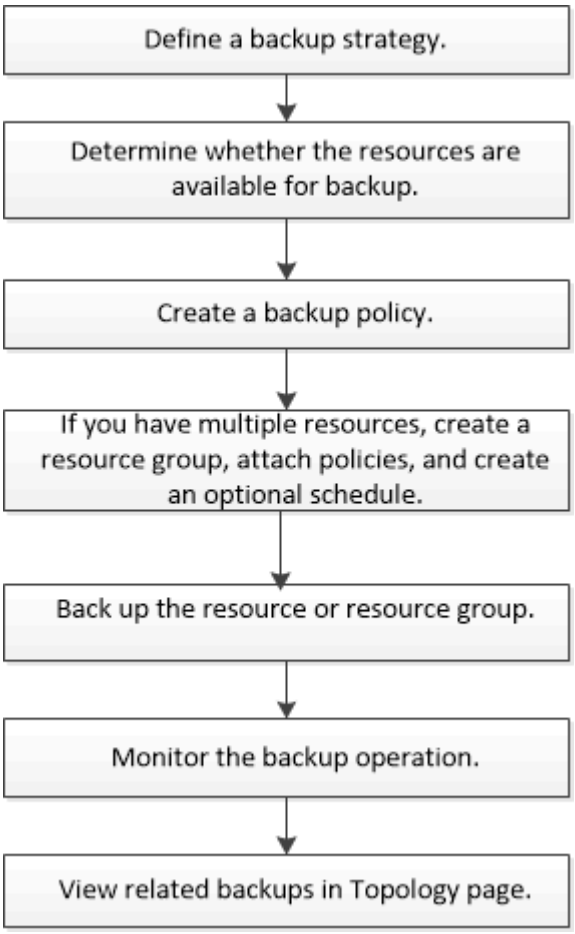
Sichern Sie Windows File-Systeme

Sichern Sie Windows File-Systeme

Wenn das SnapCenter-Plug-in für Microsoft Windows in Ihrer Umgebung installiert wird, können Sie mit SnapCenter Backups der Windows Filesysteme erstellen. Sie können ein einzelnes Dateisystem oder eine Ressourcengruppe sichern, die mehrere Dateisysteme enthält. Sie können Backups nach Bedarf oder gemäß einem definierten Schutzzeitplan erstellen.

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden. Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden.

Der folgende Workflow zeigt die Reihenfolge, in der Sie die Backup-Vorgänge durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet-Hilfe oder das "SnapCenter Software Cmdlet Referenzhandbuch" enthält detaillierte Informationen zu PowerShell Cmdlets.

Bestimmen Sie die Verfügbarkeit von Ressourcen für Windows File-Systeme

Ressourcen sind die LUNs und ähnliche Komponenten in Ihrem Dateisystem, die von Ihren installierten Plug-ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsaufträge auf mehreren

Ressourcen ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie verfügbar haben. Die Ermittlung verfügbarer Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von SVM-Verbindungen (Storage Virtual Machine) und das Hinzufügen von Anmeldeinformationen.
- Wenn Dateien auf VMware RDM-LUNs oder VMDKs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren. Weitere Informationen finden Sie unter "Dokumentation zum SnapCenter Plug-in für VMware vSphere".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **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 in den SnapCenter-Serverbestand aktualisiert.

   Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Erstellen von Backup-Richtlinien für Windows Filesysteme

Sie können eine neue Sicherungsrichtlinie für Ressourcen erstellen, bevor Sie SnapCenter zum Sichern von Windows-Dateisystemen verwenden, oder Sie können eine neue Backup-Richtlinie zum Zeitpunkt der Erstellung einer Ressourcengruppen oder beim Backup einer Ressource erstellen.

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben. "Weitere Informationen ."
- Sie müssen auf die Datensicherung vorbereitet sein.

  Zur Vorbereitung auf die Datensicherung müssen Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Erkennung von Ressourcen und das Erstellen von SVM-Verbindungen (Storage Virtual Machine) durchgeführt werden.

- Wenn Sie Snapshots auf einen sekundären gespiegelten oder Vault-Storage replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Ziel-Volumes zugewiesen haben.
- 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

- Prüfen Sie die spezifischen Voraussetzungen und Einschränkungen von SnapMirror Active Sync. Weitere

Informationen finden Sie unter "Objektgrenzen für die aktive SnapMirror Synchronisierung".

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Wenn Sie eine Snapshot-Sperrfrist festlegen, wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.
  - Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Um zu bestimmen, ob Sie eine vorhandene Richtlinie verwenden können, wählen Sie den Richtliniennamen aus und klicken Sie dann auf **Details**.

   Nach Überprüfung der vorhandenen Richtlinien können Sie eine der folgenden Aktionen durchführen:

   - Vorhandene Richtlinie verwenden
   - Kopieren Sie eine vorhandene Richtlinie, und ändern Sie die Richtlinienkonfiguration.
   - Erstellen Sie eine neue Richtlinie.
4. Um eine neue Richtlinie zu erstellen, klicken Sie auf **Neu**.
5. Geben Sie auf der Seite Name den Richtliniennamen und eine Beschreibung ein.
6. Führen Sie auf der Seite Backup-Optionen die folgenden Aufgaben aus:

   a. Wählen Sie eine Sicherungseinstellung aus.

Option	Beschreibung
Konsistentes File-System-Backup	Wählen Sie diese Option, wenn SnapCenter das Festplattenlaufwerk stilllegen soll, auf dem sich das Dateisystem befindet, bevor der Sicherungsvorgang beginnt, und setzen Sie das Laufwerk nach Abschluss des Sicherungsvorgangs wieder ein.
Crash-konsistentes Backup des File-Systems	Wählen Sie diese Option, wenn Sie nicht möchten, dass SnapCenter das Festplattenlaufwerk stilllegt, auf dem sich das Dateisystem befindet.

b. Wählen Sie eine Zeitplanfrequenz (auch als Richtlinientyp bezeichnet) aus.

   Die Richtlinie gibt nur die Backup-Häufigkeit an. Der spezifische Schutzzeitplan für das Sichern ist in der Ressourcengruppe festgelegt. Daher können zwei oder mehr Ressourcengruppen dieselbe Richtlinien- und Backup-Häufigkeit teilen, jedoch unterschiedliche Backup-Pläne haben.

ⓘ Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

7. Legen Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für On-Demand-Backups und für jede ausgewählte Zeitplanfrequenz fest.

Option	Beschreibung
Gesamtzahl der zu behaltenden Snapshot-Kopien	Wählen Sie diese Option, wenn Sie die Anzahl der Snapshot-SnapCenter-Speicher angeben möchten, bevor Sie sie automatisch löschen.
Snapshot Kopien löschen, die älter als sind	Wählen Sie diese Option, wenn Sie die Anzahl der Tage angeben möchten, die SnapCenter eine Backup-Kopie behält, bevor Sie sie löschen.
Sperrfrist von Snapshot-Kopien	Wählen Sie als Sperrzeitraum für Snapshots Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

ⓘ Sie sollten den Aufbewahrungswert auf 2 oder höher einstellen. Der Mindestwert für die Aufbewahrungsanzahl beträgt 2.

ⓘ Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.

8. Geben Sie auf der Seite „Replikation“ die Replikation auf das sekundäre Speichersystem an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu erstellen. Diese Option sollte für SnapMirror Active Sync aktiviert sein. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Siehe "Sehen Sie sich zugehörige Backups und Klone auf der Seite Topologie an".
Aktualisieren Sie die SnapVault nach dem Erstellen einer Snapshot Kopie	Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche Aktualisieren auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit, die von ONTAP abgerufen werden, aktualisiert. Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche Aktualisieren auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert. Weitere Informationen zu SnapLock Vault finden Sie unter "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel"

Für dieses Feld…	Tun Sie das…
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

9. Geben Sie auf der Seite Skript den Pfad des Prescript oder Postscript ein, den der SnapCenter-Server vor oder nach dem Backup ausführen soll, bzw. ein Zeitlimit, das SnapCenter wartet, bis das Skript ausgeführt wird, bevor das Timing out abgeschlossen wird.

   Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren und Protokolle zu senden.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

Erstellen von Ressourcengruppen für Windows-Dateisysteme

Eine Ressourcengruppe ist der Container, zu dem Sie mehrere Dateisysteme hinzufügen können, die Sie schützen möchten. Sie müssen auch eine oder mehrere Richtlinien an die Ressourcengruppe anhängen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten, und dann den Backup-Zeitplan festlegen.

Über diese Aufgabe

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

sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

- Das Hinzufügen neuer Dateisysteme ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Dateisysteme zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Status Ressourcen hinzufügen.

Schritte

1. 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 Option **Dateisysteme** aus der Liste aus.

   Wenn Sie vor Kurzem ein Dateisystem zu SnapCenter hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie Auf **Neue Ressourcengruppe**.
4. Gehen Sie auf der Seite Name im Assistenten wie folgt vor:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.
Tag	Geben Sie ein beschreibende Tag ein, um beim Suchen einer Ressourcengruppe zu helfen.

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 vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

   b. Klicken Sie im Abschnitt Verfügbare Ressourcen auf die Dateisysteme, die Sie sichern möchten, und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt Hinzufügen zu verschieben.

      Wenn Sie die Option **Autoselect alle Ressourcen auf demselben Speichervolumen** 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 **Autoselect alle Ressourcen auf demselben Speichervolumen**, und wählen Sie dann die Dateisysteme aus, die Sie in den Abschnitt Hinzufügen verschieben möchten.

6. Führen Sie auf der Seite Richtlinien die folgenden Aufgaben aus:

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

      Sie können eine beliebige vorhandene Richtlinie auswählen und auf **Details** klicken, um zu bestimmen, 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“ aufgeführt.

   b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies auf * * in der Spalte Configure Schedules für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

   c. Wenn die Richtlinie mit mehreren Terminplantypen (Frequenzen) verknüpft ist, wählen Sie die Frequenz aus, die Sie konfigurieren möchten.

   d. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **Finish** klicken.

      Die konfigurierten Zeitpläne werden in der Spalte „angewendete Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

   Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden. Sie sollten die Zeitpläne aus dem Windows Task Scheduler und dem SQL Server Agent nicht ändern.

7. Geben Sie auf der Seite Benachrichtigung wie folgt Informationen an:

Für dieses Feld…	Tun Sie das…
E-Mail-Präferenz	Wählen Sie **immer**, **bei Ausfall** oder **bei Fehlschlag oder Warnung**, um E-Mails an Empfänger zu senden, nachdem Sie Backup-Ressourcengruppen erstellt, Richtlinien angehängt und Zeitpläne konfiguriert haben. Geben Sie den SMTP-Server, die Standard-E-Mail-Betreffzeile und die E-Mail-Adressen an und von ein.
Von	E-Mail-Adresse
Bis	E-Mail-Adresse
Betreff	Standard-E-Mail-Betreffzeile

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

Sie können ein Backup nach Bedarf durchführen oder warten, bis das geplante Backup durchgeführt wird.

Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um Datensicherungsvorgänge durchzuführen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige Management-LIF-IP-Adresse verfügen.

Schritte

1. Starten Sie eine PowerShell Core-Verbindungssitzung mit dem Cmdlet "Open-SmConnection".

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

   ```
   PS C:\> Open-SmConnection
   ```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

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

Bedarfsgerechtes Backup für eine einzelne Ressource für Windows File-Systeme

Wenn sich eine Ressource nicht in einer Ressourcengruppe befindet, können Sie die Ressource On Demand auf der Seite Ressourcen sichern.

Über diese Aufgabe

Wenn Sie eine Ressource mit einer SnapMirror Beziehung zum sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Beim Backup eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount-Punkt (VMP) in dem gesicherten Dateisystem gemountet sind.

Wenn Sie in einem Windows-Dateisystemkontext arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht ein inkonsistentes Backup und ein möglicher Datenverlust beim Restore. 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).

UI von SnapCenter

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 aus, und wählen Sie dann die Ressource aus, die Sie sichern möchten.
3. Wenn der Assistent „Dateisystem – Schutz“ nicht automatisch startet, klicken Sie auf **Schützen**, um den Assistenten zu starten.

   Legen Sie die Schutzeinstellungen fest, wie in den Aufgaben zum Erstellen von Ressourcengruppen beschrieben.

4. Optional: Geben Sie auf der Seite Ressource des Assistenten ein benutzerdefiniertes Namensformat für den Snapshot ein.

   Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird an den 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 Dropdown-Liste aus.

      Sie können eine beliebige vorhandene Richtlinie auswählen und dann auf **Details** klicken, um zu bestimmen, ob Sie diese Richtlinie verwenden können.

      Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine vorhandene Richtlinie kopieren und ändern oder Sie können 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“ aufgeführt.

   b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies in der Spalte Configure Schedules für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten, auf  .

   c. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **Finish** klicken.

      Die konfigurierten Zeitpläne werden in der Spalte „angewendete Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

   "Geplante Vorgänge können fehlschlagen"

6. Führen Sie auf der Seite Benachrichtigung die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
E-Mail-Präferenz	Wählen Sie * immer* oder **bei Ausfall** oder **bei Fehlschlag oder Warnung** aus, um E-Mails an Empfänger zu senden, nachdem Sie Backup-Ressourcengruppen erstellt, Richtlinien angehängt und Zeitpläne konfiguriert haben. Geben Sie die SMTP-Serverinformationen, die Standard-E-Mail-Betreffzeile und die E-Mail-Adressen „`bis`“ und „`von`“ ein.
Von	E-Mail-Adresse
Bis	E-Mail-Adresse
Betreff	Standard-E-Mail-Betreffzeile

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

   Die Seite der Datenbanktopologie wird angezeigt.

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

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

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

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem SQL Backup-Typ von FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

In diesem Beispiel wird eine neue Backup-Richtlinie mit einem Backup-Typ von CrashConsistent für Windows File-Systeme erstellt:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Ermitteln Sie Host-Ressourcen mit dem Cmdlet "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
```

   In diesem Beispiel werden Ressourcen für Windows File-Systeme auf dem angegebenen Host ermittelt:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Fügen Sie mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter hinzu.

   In diesem Beispiel wird eine neue Ressourcengruppe für die Sicherung von SQL-Datenbanken 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"
```

   Dieses Beispiel erstellt eine neue Windows Dateisystem-Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

   In diesem Beispiel wird ein Job-Summary-Bericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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

Sichern Sie Ressourcengruppen für Windows File-Systeme

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt. Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups 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 Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts verwendet, kann der Backup-Vorgang bei einigen Hosts aufgrund von Netzwerkproblemen zu spät auslösen. Sie sollten den Wert von MaxRetryForUninitializedHosts in Web.config mit dem Cmdlet "Set-SmConfigSettings PowerShell" konfigurieren

Beim Backup eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount-Punkt (VMP) in dem gesicherten Dateisystem gemountet sind.

Wenn Sie in einem Windows-Dateisystemkontext arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht ein inkonsistentes Backup und ein möglicher Datenverlust beim Restore. 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 **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf klicken und das Tag auswählen. Sie können dann 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**.

   Wenn Sie für das SnapCenter Plug-in für Oracle Database eine föderierte Ressourcengruppe mit zwei Datenbanken haben und eine der Datenbanken Datendatei auf einem nicht-NetApp Storage besitzt, wird der Backup-Vorgang abgebrochen, obwohl sich die andere Datenbank auf einem NetApp Storage befindet.
4. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

   b. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
   - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen. Um die Größe des Java-Heaps zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript startet der `do_start method` Befehl den SnapCenter VMware Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Monitoring von Backup-Vorgängen

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

Über diese Aufgabe

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

- In Bearbeitung
- Erfolgreich abgeschlossen

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

Schritte

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

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

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

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

Überwachen Sie die Vorgänge im Teilfenster „Aktivität“

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

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

Schritte

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

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

Abbrechen von Backup-Vorgängen

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *  , um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Sehen Sie sich zugehörige Backups und Klone auf der Seite Topologie an

Wenn Sie die Erstellung von Backups oder Klonen einer Ressource vorbereiten, können Sie eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzeigen. Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Über diese Aufgabe

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

-

 Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.

-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.

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

-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.
  - Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie erstellt haben, um nur 4 Backups aufzubewahren, werden die Anzahl der angezeigten Backups 6 angezeigt.
  - Wenn Sie ein Upgrade von SnapCenter 1.1 durchgeführt haben, werden die Klone auf dem sekundären (Mirror oder Vault) nicht unter Mirror-Kopien oder Vault-Kopien in der Topologieseite angezeigt. Alle mit SnapCenter 1.1 erstellten Klone werden unter den lokalen Kopien in SnapCenter 3.0 angezeigt.

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

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

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

Schritte

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

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

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

Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone angezeigt. Nur für Oracle-Datenbanken wird im Abschnitt „Übersichtskarte“ auch die Gesamtanzahl der Protokollsicherungen angezeigt.

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

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

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

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

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

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

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

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

   Sie können Backups, die sich auf dem sekundären Speichersystem befinden, nicht umbenennen oder löschen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon in der Tabelle aus und klicken Sie auf , um ihn zu löschen.

Beispiel für Backups und Klone auf dem primären Speicher

Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets

Sie können das Cmdlet "Remove-SmBackup" verwenden, um die Anzahl der Backups für sekundäre Backups zu bereinigen, die keinen Snapshot haben. Sie können dieses Cmdlet verwenden, wenn die in der Topologie zum Verwalten von Kopien angezeigten Snapshots insgesamt nicht mit der Einstellung für die Aufbewahrung von sekundären SpeicherSnapshot übereinstimmen.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

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

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Bereinigen Sie die Anzahl der sekundären Backups mit dem Parameter -CleanupSecondaryBackups.

   In diesem Beispiel wird die Anzahl der Backups für sekundäre Backups 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"):
```

Stellen Sie Windows-Dateisysteme wieder her

Windows Dateisystemsicherungen wiederherstellen

Sie können SnapCenter verwenden, um Backups von Dateisystemen wiederherzustellen. Die Wiederherstellung des Dateisystems ist ein mehrphasiger Prozess, bei dem alle Daten von einem angegebenen Backup an den ursprünglichen Speicherort des Filesystems kopiert werden.

Bevor Sie beginnen

- Sie müssen das Dateisystem gesichert haben.
- Wenn ein geplanter Vorgang, z. B. ein Backup-Vorgang, derzeit für ein Dateisystem ausgeführt wird, muss dieser Vorgang abgebrochen werden, bevor Sie einen Wiederherstellungsvorgang starten können.
- Sie können ein Dateisystem-Backup nur am ursprünglichen Speicherort, nicht in einem alternativen Pfad wiederherstellen.

Sie können keine einzelne Datei aus einem Backup wiederherstellen, da das wiederhergestellte Dateisystem alle Daten überschreibt, die sich am ursprünglichen Speicherort des Dateisystems befinden. Zum Wiederherstellen einer einzelnen Datei aus einem Dateisystem-Backup müssen Sie das Backup klonen und auf die Datei im Klon zugreifen.

- Sie können ein System oder ein Startvolume nicht wiederherstellen.
- SnapCenter kann Filesysteme in einem Windows Cluster wiederherstellen, ohne die Cluster-Gruppe offline zu schalten.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 Ressourcengruppen aus.
3. Wählen Sie eine Ressourcengruppe aus der Liste aus, und klicken Sie dann auf **Wiederherstellen**.
4. Wählen Sie auf der Seite Backups aus, ob Sie Daten aus primären oder sekundären Speichersystemen wiederherstellen möchten, und wählen Sie dann ein Backup aus, das wiederhergestellt werden soll.
5. Wählen Sie im Assistenten Wiederherstellen Ihre Optionen aus.
6. Sie können den Pfad und die Argumente des Prescript oder Postscript eingeben, die SnapCenter vor bzw. nach der Wiederherstellung ausführen soll.

   Beispielsweise können Sie ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

7. Wählen Sie auf der Seite Benachrichtigung eine der folgenden Optionen aus:

Für dieses Feld…	Tun Sie das…
Protokollieren der Ereignisse des SnapCenter-Servers im Syslog-Storage-System	Wählen Sie diese Option aus, um SnapCenter Serverereignisse im Syslog des Speichersystems zu protokollieren.
Senden der AutoSupport-Benachrichtigung für fehlgeschlagene Vorgänge an das Storage-System	Wählen Sie diese Option aus, um Informationen zu fehlgeschlagenen Vorgängen mithilfe von AutoSupport an NetApp zu senden.
E-Mail-Präferenz	Wählen Sie **immer**, **bei Ausfall** oder **bei Fehlschlag oder Warnung** aus, um nach der Wiederherstellung von Backups E-Mail-Nachrichten an Empfänger zu senden. Geben Sie den SMTP-Server, die Standard-E-Mail-Betreffzeile und die E-Mail-Adressen an und von ein.

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

Wenn das wiederhergestellte Dateisystem eine Datenbank enthält, müssen Sie auch die Datenbank wiederherstellen. Wenn Sie die Datenbank nicht wiederherstellen, ist Ihre Datenbank möglicherweise ungültig. Informationen zum Wiederherstellen von Datenbanken finden Sie im Data Protection Guide für diese Datenbank.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

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

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

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

Überwachen von Restore-Vorgängen

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

Über diese Aufgabe

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

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

- In Bearbeitung

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

Schritte

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

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

Wiederherstellungsvorgänge abbrechen

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Nachdem Sie den Wiederherstellungsvorgang gestartet haben, klicken Sie auf  das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Klonen von Windows Filesystemen

Klonen aus einem Windows File-System-Backup

Sie können SnapCenter zum Klonen eines Windows Filesystem-Backups verwenden. Wenn Sie eine Kopie einer einzelnen Datei wünschen, die versehentlich gelöscht oder geändert wurde, können Sie ein Backup klonen und auf diese Datei im Klon zugreifen.

Bevor Sie beginnen

- Sie sollten auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von SVM-Verbindungen (Storage Virtual Machine) abschließen.
- Sie sollten eine Sicherung des Dateisystems haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Sie können keine Ressourcengruppe klonen. Sie können nur individuelle File-System-Backups klonen.
- Wenn sich ein Backup auf einer virtuellen Maschine mit VMDK-Laufwerk befindet, kann SnapCenter das Backup nicht auf einem physischen Server klonen.
- Wenn Sie ein Windows Cluster klonen (z. B. eine gemeinsame LUN oder ein gemeinsam genutztes Cluster-Volume (CSV)-LUN), wird der Klon als dedizierte LUN auf dem von Ihnen angegebenen Host gespeichert.
- Für einen Klonvorgang kann das Stammverzeichnis des Volume-Bereitstellungspunkts kein freigegebenes Verzeichnis sein.
- Auf einem Node, der nicht der Home-Node für das Aggregat ist, können Sie keinen Klon erstellen.
- Sie können keine wiederkehrenden Vorgänge des Klons (Lebenszyklus von Klonen) für Windows Filesysteme planen, sondern nur Backups nach Bedarf klonen.
- Wenn Sie eine LUN verschieben, die einen Klon enthält, auf ein neues Volume, kann SnapCenter den Klon nicht mehr unterstützen. Beispielsweise können Sie diesen Klon nicht mit SnapCenter löschen.

- Sie können nicht über mehrere Umgebungen hinweg klonen. Zum Beispiel Klonen von einer physischen Festplatte auf eine virtuelle Festplatte oder umgekehrt.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

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

UI von SnapCenter

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 Option **Dateisysteme** aus der Liste aus.
3. Wählen Sie den Host aus.

   Die Topologieansicht wird automatisch angezeigt, wenn die Ressource geschützt ist.

4. Wählen Sie in der Liste Ressourcen das zu klonenden Backup aus, und klicken Sie dann auf das Klon-Symbol.
5. Gehen Sie auf der Seite Optionen wie folgt vor:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie den Host aus, auf dem der Klon erstellt werden soll.
„Automatische Zuweisung von Bereitstellungspunkt“ oder „Automatische Zuweisung von Volume-Bereitstellungspunkt unter Pfad“	Legen Sie fest, ob unter einem Pfad automatisch ein Mount-Punkt oder ein Volume-Mount-Punkt zugewiesen werden soll. Automatisches Zuweisen von Volume-Mount-Punkt unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht es Ihnen, ein bestimmtes Verzeichnis bereitzustellen, in dem die Mount-Punkte erstellt werden. Bevor Sie diese Option auswählen, müssen Sie überprüfen, ob das Verzeichnis leer ist. Wenn ein Backup im Verzeichnis vorhanden ist, befindet sich das Backup nach dem Mount-Vorgang in einem ungültigen Status.
Speicherort der Archivierung	Wählen Sie einen Archivort aus, wenn Sie ein sekundäres Backup klonen.

6. Geben Sie auf der Seite Skript alle Druckschriften oder Postskripte an, die Sie ausführen möchten.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Backups auf, die mit dem Cmdlet "Get-SmBackup" oder "Get-SmResourceGroup" geklont werden können.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   In diesem Beispiel werden Informationen über eine bestimmte Ressourcengruppe, ihre Ressourcen und zugehörige 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}
HostResourceMaping : {}
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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup mit dem Cmdlet "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 für eine angegebene 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 Clone-Jobs mit dem Cmdlet Get-SmCloneReport an.

   In diesem Beispiel wird ein Klonbericht für die angegebene Job-ID angezeigt:

```
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}
```

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

Monitoring von Klonvorgängen

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

Über diese Aufgabe

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

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

Schritte

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

Klonvorgänge abbrechen

Sie können Klonvorgänge in die Warteschlange abbrechen.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Klonvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Klonvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen ausgeführten Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Klonvorgänge abzubrechen.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Vorgang aus, und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Klonvorgangs auf  das Teilfenster „Aktivität“, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite **Job Details** auf **Job abbrechen**.

Teilen Sie einen Klon auf

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

Über diese Aufgabe

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

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

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

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

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

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

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

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

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

   Beispiel:

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

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

Verwandte Informationen

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

Schutz von 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 Host-seitige Komponente der NetApp SnapCenter Software, die das Management der applikationsspezifischen Datensicherung von Exchange Datenbanken ermöglicht. Das Plug-in für Exchange automatisiert Backup und Restore von Exchange Datenbanken in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für Exchange installiert ist, können Sie mithilfe von SnapCenter mit NetApp SnapMirror Technologie gespiegelte Kopien von Backups auf einem anderen Volume erstellen. In diesem Fall ermöglicht NetApp SnapVault Technologie eine Disk-to-Disk-Backup-Replizierung, um Standard-Compliance- oder Archivierungszwecke zu erfüllen.

Wenn Sie E-Mails oder Mailboxen statt der gesamten Exchange Datenbank wiederherstellen möchten, können Sie die Single Mailbox Recovery (SMBR) Software verwenden. Die Einstellung der Verfügbarkeit für NetApp Single Mailbox Recovery (EOA) steht am 12. Mai 2023 fest. NetApp unterstützt Kunden, die für den Zeitraum der Support-Berechtigung Mailbox-Kapazität, Wartung und Support erworben haben, weiterhin über die am 24. Juni 2020 eingeführten Marketing-Teilenummern.

NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. OnTrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können von Ontrack (bis licensingteam@ontrack.com) neue Ontrack PowerControls Softwarelizenzen und Ontrack PowerControls Wartungs- und Supportverlängerungen für eine granulare Mailbox-Recovery erwerben.

Das Plug-in für Exchange unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]). Damit können Business-Services auch bei einem vollständigen Standortausfall weiterlaufen und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.

Er unterstützt den asymmetrischen Modus, Failover oder nicht-Duplex-Modus von SnapMirror Active Sync. Dies bezieht sich auf die Lösung, bei der sich der optimierte Pfad nur vom primären LUN-Besitzknoten befindet. Sämtliche I/O-Vorgänge, die auf den sekundären Cluster-Pfaden eingehen, werden von Proxying zum primären Cluster. Die synchrone Replizierung ist unidirektional und bewegt sich in Richtung des primären zu des sekundären.

Ihre Möglichkeiten mit dem SnapCenter Plug-in für Microsoft Exchange Server

Mit dem Plug-in für Exchange können Sie Exchange Server Datenbanken sichern und wiederherstellen.

- Überwachen und managen Sie aktive Bestände an Exchange Database Availability Groups (DAGs), Datenbanken und Replikatsets

- Definition von Richtlinien mit den Sicherungseinstellungen für die Backup-Automatisierung
- Weisen Sie den Ressourcengruppen Richtlinien zu
- Sicherung einzelner DAGs und Datenbanken
- Backup von primären und sekundären Exchange Mailbox-Datenbanken
- Wiederherstellung von Datenbanken aus primären und sekundären Backups

Storage-Typen, die von SnapCenter Plug-in für Microsoft Windows und für Microsoft Exchange Server unterstützt werden

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines. Sie müssen überprüfen, ob Ihr Speichertyp unterstützt wird, bevor Sie das Paket für Ihren Host installieren.

SnapCenter Provisioning und Datensicherung werden unter Windows Server unterstützt. Die neuesten Informationen zu unterstützten Versionen finden Sie im https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT [NetApp Interoperabilitäts-Matrix-Tool^].

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische SnapCenter Benutzeroberfläche (GUI) oder PowerShell Commandlets	
Physischer Server	ISCSI-verbundene LUNs	SnapCenter GUI oder PowerShell Commandlets	
VMware VM	RDM-LUNs, die über einen FC- oder iSCSI-HBA verbunden sind	PowerShell Commandlets	Nur physische Kompatibilität VMDKs werden nicht unterstützt.
VMware VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	VMDKs werden nicht unterstützt.

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	Virtuelle FC-LUNs (VFC), die über einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Sie müssen Hyper-V Manager verwenden, um virtuelle FC (VFC) LUNs bereitzustellen, die über einen virtuellen Fibre Channel Switch verbunden sind. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.
Hyper-V VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Minimale ONTAP-Berechtigungen, die für das Exchange Plug-in erforderlich sind

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher

- Event Generate-AutoSupport-log
- Job-Verlauf wird angezeigt
- Job beenden
- lun
- lun erstellen
- lun erstellen
- lun erstellen
- lun löschen
- lun Initiatorgruppe hinzufügen
- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele

- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen
- Show-Disk-Nutzung für Volume-Dateien
- Volume ist offline
- Das Volume ist online
- Volume-Änderung
- Erstellen von Volume-qtree
- Volume qtree löschen
- Änderung des Volume-qtree
- Volume-qtree anzeigen
- Volume-Einschränkung
- Volumen anzeigen
- Erstellen von Volume-Snapshots
- Volume Snapshot löschen
- Ändern des Volume-Snapshots
- Volume Snapshot modify-snaplock-expiry-time
- Umbenennung von Volume-Snapshots
- Wiederherstellung von Volume Snapshots
- Restore-Datei für Volume Snapshots
- Volume-Snapshot werden angezeigt
- Volume-Aufhängung nicht verfügbar
- cifs von vserver
- erstellung von cifs-Freigaben von vserver
- cifs-Freigabe von vserver: Löschen
- vserver cifs shadowcopy anzeigen
- cifs-Freigabe von vserver wird angezeigt
- vserver cifs zeigen
- vserver Exportrichtlinie
- Erstellung von vserver Exportrichtlinien
- vserver: Löschen der Exportrichtlinie
- Erstellung von vserver Export-Policy-Regel

- vserver: Export-Policy-Regel anzeigen
- vserver Export-Policy wird angezeigt
- vserver iscsi
- vserver iscsi-Verbindung wird angezeigt
- vserver zeigen

- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle wird angezeigt
  - vserver

Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

> Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

> SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie für Exchange Server-Ressourcen definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, können Sie sicherstellen, dass Sie über die Backups verfügen, die Sie benötigen, um Ihre Datenbanken erfolgreich wiederherzustellen. Ihre Backup-Strategie wird durch Ihre Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) weitgehend bestimmt.

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich

Verfügbarkeit und Performance des Service. Die RTO ist der Zeitpunkt, zu dem ein Geschäftsprozess nach einer Service-Unterbrechung wiederhergestellt werden muss. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Backup-Strategie bei.

Arten von Backups, die für Exchange-Datenbank unterstützt werden

Für das Backup von Exchange Mailboxen mit SnapCenter müssen Sie den Ressourcentyp auswählen, beispielsweise Datenbanken und Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAG). Mithilfe der Snapshot Technologie werden schreibgeschützte Online-Kopien der Volumes erstellt, auf denen sich die Ressourcen befinden.

Backup-Typ	Beschreibung
Vollständiges Backup und Backup für Protokolle	Backups der Datenbanken und aller Transaktions-Logs, einschließlich der gekürzten Logs. Nach Abschluss eines vollständigen Backups schneidet der Exchange Server die Transaktions-Logs ab, die bereits in die Datenbank übernommen wurden. Normalerweise sollten Sie diese Option wählen. Wenn Ihre Backup-Zeit jedoch kurz ist, können Sie wählen, keine Transaktions-Log-Backup mit vollständiger Sicherung auszuführen.
Vollständiges Backup	Sicherung von Datenbanken und Transaktionsprotokollen. Die gekürzten Transaktionsprotokolle werden nicht gesichert.
Backup-Protokollierung	Sichert alle Transaktions-Logs. Die gekürzten Protokolle, die bereits in die Datenbank geschrieben sind, werden nicht gesichert. Wenn Sie regelmäßige Transaktions-Log-Backups zwischen vollständigen Datenbank-Backups planen, können Sie granulare Recovery-Punkte auswählen.

Backup-Pläne für Datenbank-Plug-ins

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall

fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen. So könnten beispielsweise regelmäßige Transaktions-Log-Backups ausreichen, um sicherzustellen, dass Sie die Backups haben, die Sie benötigen. Je öfter Sie Ihre Datenbanken sichern, desto weniger Transaktions-Logs benötigt SnapCenter zum Zeitpunkt der Wiederherstellung, was zu schnelleren Restore-Vorgängen führen kann.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, für die eine Richtlinie für wöchentliche Backups konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Datenbanken erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Konventionen bei Backup-Namen

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Wie lange dauert die Speicherung von Transaktions-Log-Backups auf dem Quell-Storage Volume für Exchange Server

Das SnapCenter Plug-in für Microsoft Exchange Server benötigt Transaktions-Log-Backups, um minutengenaue Restore-Vorgänge durchzuführen, bei denen Ihre Datenbank zwischen zwei vollständigen Backups wiederhergestellt wird.

Beispiel: Wenn das Plug-in für Exchange um 8:00 Uhr ein vollständiges Backup des Transaktionsprotokolls und um 5:00 Uhr ein weiteres vollständiges Backup des Transaktionsprotokolls erstellt hat, es könnte die letzte Transaktionsprotokoll-Sicherung verwenden, um die Datenbank jederzeit zwischen 8:00 und 5:00 Uhr wiederherzustellen. wenn Transaktionsprotokolle nicht verfügbar sind, kann Plug-in für Exchange nur Point-in-Time-Wiederherstellungsvorgänge durchführen. die eine Datenbank so lange wiederherstellen, wie Plug-in für Exchange ein vollständiges Backup abgeschlossen hat.

In der Regel erfordern Sie minutengenaue Restore-Vorgänge nur für einen oder zwei Tage. SnapCenter speichert standardmäßig mindestens zwei Tage.

Festlegen einer Restore-Strategie für Exchange-Datenbanken

Durch die Definition einer Wiederherstellungsstrategie für Exchange Server können Sie Ihre Datenbank erfolgreich wiederherstellen.

Quellen für eine Wiederherstellung in Exchange Server

Sie können eine Exchange Server Datenbank aus einer Backup-Kopie im Primärspeicher wiederherstellen.

Sie können Datenbanken nur aus dem Primärspeicher wiederherstellen.

Arten von Wiederherstellungsvorgängen, die für Exchange Server unterstützt werden

Mit SnapCenter können Sie verschiedene Arten von Restore-Vorgängen für Exchange Ressourcen ausführen.

- Wiederherstellung im Minutenschnoch
- Wiederherstellung auf einen früheren Zeitpunkt

Führen Sie Wiederherstellungen minutengenau durch

In einem up-to-the-minute-Wiederherstellungsvorgang werden Datenbanken bis zu dem Punkt des Ausfalls wiederhergestellt. SnapCenter erreicht dies durch folgende Sequenz:

1. Stellt die Datenbanken aus dem vollständigen Datenbank-Backup wieder her, das Sie auswählen.
2. Wendet alle gesicherten Transaktionsprotokolle sowie alle neuen Protokolle an, die seit dem letzten Backup erstellt wurden.

   Transaktionsprotokolle werden nach vorne verschoben und auf alle ausgewählten Datenbanken angewendet.

   Exchange erstellt nach Abschluss einer Wiederherstellung eine neue Protokollkette.

   Best Practice: Es wird empfohlen, nach Abschluss einer Wiederherstellung ein neues vollständiges Backup durchzuführen und zu protokollieren.

   Für eine minutengenaue Wiederherstellung ist ein zusammenhängender Satz von Transaktionsprotokollen erforderlich.

   Nach der Durchführung eines up-to-the-minute-Restores ist das Backup, das Sie für die Wiederherstellung verwendet haben, nur für zeitpunktgenaue Restore-Vorgänge verfügbar.

   Wenn Sie keine up-to-the-minute-Wiederherstellung für alle Backups benötigen, können Sie die Transaktions-Log-Backup-Aufbewahrung Ihres Systems mithilfe der Backup-Richtlinien konfigurieren.

Wiederherstellung auf einen früheren Zeitpunkt

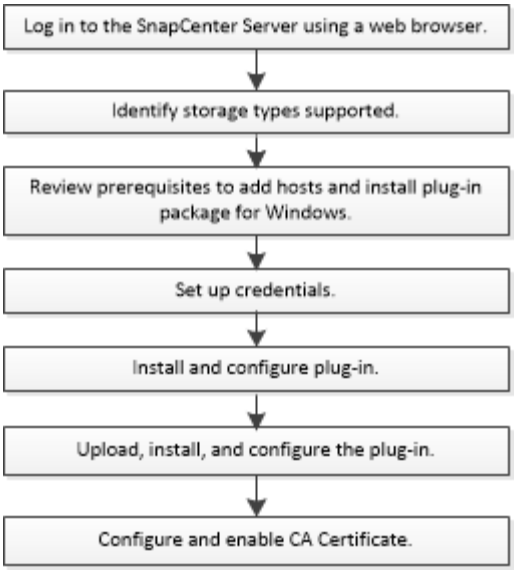
In einer zeitpunktgenauen Restore-Operation werden Datenbanken nur auf eine bestimmte Zeit aus der Vergangenheit wiederhergestellt. Ein Point-in-Time-Wiederherstellungsvorgang findet in den folgenden Situationen statt:

- Die Datenbank wird zu einem bestimmten Zeitpunkt in einem gesicherten Transaktions-Log wiederhergestellt.
- Die Datenbank ist wiederhergestellt, und nur ein Teil der gesicherten Transaktions-Logs wird angewendet.

Installieren Sie das SnapCenter Plug-in für Microsoft Exchange Server

Installations-Workflow 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 für das Hinzufügen von Hosts und die Installation 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 mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Sie müssen Microsoft Exchange Server 2013, 2016 oder 2019 für Standalone- und Database Availability Group-Konfigurationen verwenden.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen über einen Benutzer mit Administratorrechten auf dem Exchange Server verfügen.
- Wenn SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, müssen Sie den von SnapDrive für Windows verwendeten VSS Hardware Provider deinstallieren, bevor Sie Plug-in für Exchange auf demselben Exchange-Server installieren, um den erfolgreichen Datenschutz mit SnapCenter zu gewährleisten.
- Wenn SnapManager für Microsoft Exchange Server und das Plug-in für Exchange auf demselben Server installiert sind, müssen Sie alle vom SnapManager für Microsoft Exchange Server erstellten Zeitpläne aussetzen oder löschen.
- Der Host muss auf den vollständig qualifizierten Domänennamen (FQDN) vom Server resolable sein. Wenn die Hosts-Datei geändert wird, damit sie resolable ist und wenn sowohl der Kurzname als auch der FQDN in der Datei Hosts angegeben sind, erstellen Sie einen Eintrag in der Datei SnapCenter Hosts im folgenden Format: *<ip_Address> <Host_fqdn> <Host_Name>*.
- Stellen Sie sicher, dass die folgenden Ports in der Firewall nicht blockiert sind, da sonst der Vorgang zum Hinzufügen eines Hosts fehlschlägt. Um dieses Problem zu lösen, müssen Sie den dynamischen Portbereich konfigurieren. Weitere Informationen finden Sie unter "Microsoft-Dokumentation".

- Port-Bereich 50000 - 51000 für Windows 2016 und Exchange 2016
- Port-Bereich 6000 - 6500 für Windows 2012 R2 und Exchange 2013
- Portbereich 49152 - 65536 für Windows 2019

Führen Sie die folgenden Befehle aus, um den Port-Bereich zu identifizieren:

- 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 für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Berechtigungen für Exchange Server erforderlich

Damit SnapCenter das Hinzufügen von Exchange Server oder DAG sowie die Installation des SnapCenter Plug-ins für Microsoft Exchange Server auf einem Host oder einer DAG aktivieren kann, müssen Sie SnapCenter mit Anmeldedaten für einen Benutzer mit einem Minimum an Berechtigungen und Berechtigungen konfigurieren.

Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten verfügen, und über lokale Anmeldeberechtigungen auf dem entfernten Exchange-Host sowie über Administratorberechtigungen auf allen Knoten in der DAG. Der Domänenbenutzer benötigt die folgenden Mindestberechtigungen:

- Add-MailboxDatabaseCopy
- Datenbank Entmounten
- Get-AdServerSettings
- Get-DatabaseVerfügbarkeitGroup
- Get-ExchangeServer
- Get-Mailboxdatenbank
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistik
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatenbank
- Move-DatabasePath - KonfigurationNur: €true
- Mount-Datenbank
- Neue Postboxdatenbank
- New-PublicFolderDatabase
- Mailboxdatenbank entfernen
- Entfernen Sie-MailboxDatabaseCopy
- Entfernen Sie die-PublicFolderDatabase

- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-mailboxdatenbank -allowfilerestore: €true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Richten Sie die Anmeldeinformationen für das SnapCenter-Plug-in für Windows ein

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation des Plug-in-Pakets und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken erstellen.

Über diese Aufgabe

Sie müssen Anmeldedaten für die Installation von Plug-ins auf Windows-Hosts einrichten. Obwohl Sie nach der Implementierung von Hosts und der Installation von Plug-ins Anmeldedaten für Windows erstellen können, sollten Sie vor der Implementierung von Hosts und Plug-ins zunächst die Anmeldedaten nach dem Hinzufügen von SVMs erstellen.

Richten Sie die Anmeldedaten mit Administratorrechten ein, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.

   Das Fenster Credential wird angezeigt.

4. Gehen Sie auf der Seite Credential wie folgt vor:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen ein, der für die Authentifizierung verwendet wird. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld Benutzername lautet: `UserName`
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierung	Wählen Sie Windows als Authentifizierungsmodus aus.

5. Klicken Sie auf **OK**.

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Fügen Sie Hosts hinzu und installieren Sie das Plug-in für Exchange

Sie können die Seite SnapCenter Add Host 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 ein 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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Plug-in-Installations- und Deinstallationsberechtigungen verfügt, wie z. B. die SnapCenter-Admin
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Der Nachrichtenwarteschlange-Service muss ausgeführt werden.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2016 oder höher für Microsoft Exchange Server".

Über diese Aufgabe

- 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 für einen einzelnen Host oder Cluster installieren.
- Ist ein Exchange-Knoten Teil einer DAG, kann der SnapCenter-Server nicht nur einen Knoten hinzufügen.
- Wenn Sie Plug-ins auf einem Cluster (Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert, selbst wenn einige Knoten keine Datenbanken auf NetApp LUNs haben.

Ab SnapCenter 4.6 unterstützt SCE die Mandantenfähigkeit und Sie können einen Host über die folgenden Methoden hinzufügen:

Fügen Sie einen Host-Vorgang hinzu	4.5 und früher	4.6 und höher
Fügen Sie IP-lose DAG in einer anderen Domäne oder anderen Domäne hinzu	Nicht unterstützt	Unterstützt
Fügen Sie mehrere IP-DAGs mit eindeutigen Namen hinzu. Diese befinden sich in derselben oder in mehreren Domänen	Unterstützt	Unterstützt
Fügen Sie mehrere IP- oder IP-lose DAGs mit denselben Host-Namen und/oder DB-Namen in Cross-Domain hinzu	Nicht unterstützt	Unterstützt
Hinzufügen mehrerer IP/IP-loser DAGs mit demselben Namen und domänenübergreifender	Nicht unterstützt	Unterstützt
Fügen Sie mehrere Standalone-Hosts mit demselben Namen und domänenübergreifender Infrastruktur hinzu	Nicht unterstützt	Unterstützt

Plug-in für Exchange hängt vom SnapCenter Plug-ins-Paket für Windows ab, die Versionen müssen identisch sein. Während der Installation von Plug-in für Exchange wird das SnapCenter Plug-ins Paket für Windows standardmäßig ausgewählt und zusammen mit dem VSS-Hardwareanbieter installiert.

Falls SnapManager für Microsoft Exchange Server und SnapDrive für Windows bereits installiert sind, Und Sie möchten Plug-in für Exchange auf demselben Exchange-Server installieren, müssen Sie den von SnapDrive für Windows verwendeten VSS Hardware-Anbieter deaktivieren, da er mit dem VSS Hardware Provider, der mit Plug-in für Exchange und SnapCenter Plug-ins Package für Windows installiert ist, nicht kompatibel ist. 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. Vergewissern Sie sich, dass **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie als Hosttyp * Windows* aus. SnapCenter Server fügt den Host hinzu und installiert dann auf dem Host das Plug-in für Windows und das Plug-in für Exchange, falls sie nicht bereits installiert sind. Plug-in für Windows und Plug-in für Exchange müssen die gleiche Version sein. Wenn zuvor eine andere Version des Plug-ins für Windows installiert wurde, aktualisiert SnapCenter die Version als Teil der Installation.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den vollständig qualifizierten Domänennamen (FQDN) einzugeben. Eine IP-Adresse wird nur für nicht vertrauenswürdige Domänenhosts unterstützt, wenn sie auf den FQDN auflöst. Wenn Sie einen Host mit SnapCenter hinzufügen und dieser Teil einer Unterdomäne ist, müssen Sie den FQDN angeben. Sie können IP-Adressen oder den FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Exchange DAG Vorteile einer Exchange DAG: ◦ Fügen Sie eine DAG hinzu, indem Sie den DAG-Namen, die DAG-IP-Adresse, den Node-Namen oder die Node-IP-Adresse angeben. ◦ Fügen Sie den DAG-Cluster ohne IP hinzu, indem Sie die IP-Adresse oder den FQDN eines der DAG-Cluster-Nodes angeben. ◦ Fügen Sie IP-lose DAG hinzu, die sich in derselben Domäne oder einer anderen Domäne befindet. Sie können auch mehrere IP/IP-basierte DAGs mit demselben Namen und aber verschiedenen Domänen hinzufügen. Für einen eigenständigen Host oder eine Exchange-DAG (domänenübergreifend oder gleiche Domäne) wird empfohlen, FQDN oder die IP-Adresse des Hosts oder der DAG bereitzustellen.

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

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Wenn Sie Plug-in für Exchange auswählen, wird das SnapCenter-Plug-in für Microsoft SQL Server automatisch deaktiviert. Microsoft empfiehlt, dass SQL Server und Exchange-Server aufgrund der verwendeten Speichermenge und anderer von Exchange benötigten Ressourcen nicht auf demselben System installiert werden.

6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Installationspfad	Der Standardpfad ist `C:\Program Files\NetApp\SnapCenter`. Optional können Sie den Pfad anpassen.
Fügen Sie alle Hosts in der DAG hinzu	Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine DAG hinzufügen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: *Domainname\AccountName€*. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird der Host validiert, um zu bestimmen, ob er die Anforderungen für die Installation des Plug-ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden die entsprechenden Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit Speicherplatz oder RAM zusammenhängt, können Sie die Datei Web.config in WebApp aktualisieren `C:\Program Files\NetApp\SnapCenter` , 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. Überwachen Sie den Installationsfortschritt.

Konfigurieren Sie den benutzerdefinierten Port für die NET TCP-Kommunikation

Standardmäßig verwendet das SnapCenter-Plug-in für Windows ab SnapCenter 6.0 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:\Program Files\NetApp\SnapCenter\SnapCenter*

Plug-in für Microsoft Windows\vssprovidern\navssprv.exe.config auf die erforderliche Portnummer.
`<add key="NetTCPPort" value="new_port_number" />`

2. Ändern Sie den Wert des Schlüssels *NetTCPPort* unter *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in für Microsoft Windows\SnapDriveService.dll.config* auf die erforderliche Port-Nummer.
`<add key="NetTCPPort" value="new_port_number" />`
3. Heben Sie die Registrierung des Services *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`

   Vergewissern Sie sich, dass der Dienst nicht in der Liste der Dienste in *Services.msc* angezeigt wird.
4. Registrieren Sie den Service *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 *Plug-in für Windows*-Dienst neu.

Installieren Sie das Plug-in für Exchange über den SnapCenter Server Host mithilfe von PowerShell Cmdlets

Sie sollten das Plug-in für Exchange über die SnapCenter-Benutzeroberfläche 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 worden sein.
- Sie müssen ein lokaler Administrator auf dem Host oder ein Benutzer mit Administratorrechten sein.
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen Plug-in, Installation und Deinstallation verfügt, wie z. B. SnapCenter Admin
- Vor der Installation des Plug-ins für Exchange müssen Sie die Installationsanforderungen und die Typen der unterstützten Konfigurationen geprüft haben.
- Der Host, auf dem das Plug-in für Exchange installiert werden soll, muss ein Windows-Host sein.

Schritte

1. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, und geben Sie dann Ihre Anmeldeinformationen ein.
2. Fügen Sie den Host hinzu, auf dem Sie das Plug-in für Exchange installieren möchten, mit dem Cmdlet *Add-SmHost* mit den erforderlichen Parametern.

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

   Es kann sich dabei um einen Standalone-Host oder eine DAG handeln. Wenn Sie eine DAG angeben, ist der Parameter *-IsDAG* erforderlich.

3. Installieren Sie das Plug-in für Exchange mit dem Cmdlet *Install-SmHostPackage* mit den erforderlichen Parametern.

   Dieser Befehl installiert das Plug-in für Exchange auf dem angegebenen Host und registriert dann das Plug-in mit SnapCenter.

Installieren Sie das SnapCenter Plug-in für Exchange im Hintergrund über die Befehlszeile

Sie sollten Plug-in für Exchange über die Benutzeroberfläche von SnapCenter installieren. Wenn Sie jedoch aus irgendeinem Grund nicht in der Lage sind, das Installationsprogramm Plug-in for Exchange unbeaufsichtigt im Silent-Modus von der Windows-Befehlszeile aus auszuführen.

Bevor Sie beginnen

- Sie müssen Ihre Microsoft Exchange Server-Ressourcen gesichert haben.
- Sie müssen die SnapCenter-Plug-in-Pakete installiert haben.
- Vor der Installation müssen Sie die frühere Version des SnapCenter-Plug-ins für Microsoft SQL Server löschen.

  Weitere Informationen finden Sie unter "So installieren Sie ein SnapCenter-Plug-in manuell und direkt über den Plug-in-Host".

Schritte

1. Überprüfen Sie, ob der Ordner *C:\temp* auf dem Plug-in-Host vorhanden ist und der angemeldete Benutzer vollständigen Zugriff darauf hat.
2. Laden Sie das SnapCenter Plug-in für Microsoft Windows von *C:\ProgramData\NetApp\SnapCenter\Paket* Repository herunter.

   Auf diesen Pfad kann von dem Host 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 zum Verzeichnis, in das 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_Path>“ BI_SERVICEACCOUNT=<Domain\<Administrator> BI_SERVICECEPWD= SCHEICE= SCHEINSW

   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\\BI_SERVICECOUNT,SPERW_Administrator,SPEICEICE_DER_DER_SPREN,SnapCenter,SCEICEICEICHTE_DER_DER_DER_DER_Administrator_SPREN,SPREN

Alle während der Installation von Plug-in für Exchange übergebenen Parameter gelten bei der Groß-/Kleinschreibung.

Geben Sie die folgenden Werte für die Variablen ein:

Variabel	Wert
/Debuglog"<Debug_Log_Path>	Geben Sie den Namen und den Speicherort der Protokolldatei für das Installationsprogramm der Suite an, wie im folgenden Beispiel: *Setup.exe /debuglog„C:\PathToLog\setupexe.log*
BI_SNAPCENTER_PORT	Geben Sie den Port an, auf dem SnapCenter mit SMCore kommuniziert.
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis für das Host-Plug-in-Paket an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter-Plug-in für das Web-Service-Konto von Microsoft Windows an.
BI_SERVICEPWD	Geben Sie das Passwort für das SnapCenter-Plug-in für das Microsoft Windows-Webservice-Konto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host implementiert werden soll.

6. Überwachen Sie den Windows Task Scheduler, die Hauptinstallationsprotokolldatei *C:\Installdebug.log* und die zusätzlichen Installationsdateien in *C:\Temp*.
7. Überwachen Sie das Verzeichnis *%temp%*, um zu überprüfen, ob die Installer *msiexe.exe* die Software fehlerfrei installieren.

Die Installation des Plug-ins für Exchange registriert das Plug-in auf dem Host und nicht auf dem SnapCenter-Server. Sie können das Plug-in auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Nach dem Hinzufügen des Hosts wird das Plug-in automatisch erkannt.

Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets

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

Über diese Aufgabe

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

- In Bearbeitung

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

Schritte

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

> Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:

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 **Miniaturdruck**.

d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.

e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:

a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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"
```

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Konfigurieren Sie SnapManager 7.x für Exchange und SnapCenter, um koexistieren zu können

Damit das SnapCenter Plug-in für Microsoft Exchange Server gemeinsam mit SnapManager für Microsoft Exchange Server eingesetzt werden kann, müssen Sie das SnapCenter Plug-in für Microsoft Exchange Server auf demselben Exchange Server

installieren, auf dem SnapManager für Microsoft Exchange Server installiert ist, indem Sie die Zeitpläne für SnapManager für Exchange deaktivieren. Und neue Zeitpläne und Backups mit dem SnapCenter Plug-in für Microsoft Exchange Server konfigurieren.

Bevor Sie beginnen

- SnapManager für Microsoft Exchange Server und SnapDrive für Windows sind bereits installiert und Backups von SnapManager für Microsoft Exchange Server sind im System und im SnapInfo Verzeichnis vorhanden.
- Sie sollten die von SnapManager für Microsoft Exchange Server erstellten Backups gelöscht oder zurückgewonnen haben, die Sie nicht mehr benötigen.
- Sie sollten alle Zeitpläne ausgesetzt oder gelöscht haben, die von SnapManager für Microsoft Exchange Server aus dem Windows-Scheduler erstellt wurden.
- Das SnapCenter Plug-in für Microsoft Exchange Server und SnapManager für Microsoft Exchange Server können parallel auf demselben Exchange Server eingesetzt werden. Sie können jedoch kein Upgrade von bestehenden SnapManager für Microsoft Exchange Server Installationen auf SnapCenter durchführen.

  SnapCenter bietet keine Upgrade-Option.

- 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 Backup von SnapManager für Microsoft Exchange Server wiederherstellen möchten, müssen Sie weitere Schritte durchführen.

Schritte

1. Bestimmen Sie mithilfe von PowerShell auf allen DAG-Knoten, ob der SnapDrive für Windows VSS Hardware Provider 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. Aus dem SnapDrive-Verzeichnis den VSS Hardware Provider von SnapDrive für Windows: *navssprv.exe -r Service -U*
3. Überprüfen Sie, ob der VSS Hardware Provider 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 SnapCenter-Plug-in für Microsoft Windows-Verzeichnis 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. Beenden Sie die Backup-Zeitpläne für SnapManager für Microsoft Exchange Server.
7. Erstellen Sie über die GUI von SnapCenter 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 nicht jetzt deinstallieren und später ein Backup von SnapManager für Microsoft Exchange Server wiederherstellen möchten:

   a. Heben Sie das SnapCenter Plug-in 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. Aus dem Verzeichnis *C:\Programme\NetApp\SnapDrive* registrieren Sie SnapDrive für Windows auf allen DAG Knoten: *navssprv.exe -r Service -a hostname\\username -p password*

Installieren Sie das SnapCenter Plug-in für VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

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

Konfigurieren Sie die CRL-Datei

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

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

jede CRL überprüft.

Bereiten Sie sich auf die Datensicherung vor

Bevor Sie Datensicherungsvorgänge wie Backup-, Klon- oder Restore-Vorgänge durchführen, müssen Sie Ihre Strategie definieren und die Umgebung festlegen. Sie können den SnapCenter Server auch zur Verwendung von SnapMirror und SnapVault Technologie einrichten.

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

Weitere Informationen

"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.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich bei SnapCenter an.
- Konfigurieren Sie die SnapCenter-Umgebung, indem Sie Storage-Systemverbindungen hinzufügen oder zuweisen und Anmeldedaten erstellen.

  SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede von SnapCenter unterstützte SVM muss über einen eindeutigen Namen verfügen.

- Fügen Sie Hosts hinzu, installieren Sie das SnapCenter Plug-in für Microsoft Windows und das SnapCenter Plug-in für Microsoft Exchange Server und ermitteln Sie die Ressourcen (aktualisieren).
- Führen Sie die Host-seitige Storage-Bereitstellung 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 für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren. Die Dokumentation zum SnapCenter Plug-in für VMware vSphere enthält weitere Informationen.

  VMDKs werden nicht unterstützt.

- Verschieben Sie eine vorhandene Microsoft Exchange Server-Datenbank von einem lokalen Laufwerk auf unterstützten Speicher mithilfe von Microsoft Exchange-Tools.
- Richten Sie SnapMirror- und SnapVault-Beziehungen ein, falls Sie eine Backup-Replizierung möchten.

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von

SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für SnapCenter 4.3.x-Anwender enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.3 Informationen zum Schutz virtualisierter Datenbanken und Filesysteme mithilfe des Linux-basierten SnapCenter Plug-ins für VMware vSphere Virtual Appliance (Open Virtual Appliance Format).

"Dokumentation zum SnapCenter Plug-in für VMware vSphere"

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von Exchange Server verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit den durchzustellenden Backup-, Restore- und erneuten Seeding-Operationen zu verstehen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind typischerweise Mailbox-Datenbanken oder Microsoft Exchange Database Availability Group (DAG), die Sie mit SnapCenter sichern.
- Eine SnapCenter Ressourcengruppe ist eine Ansammlung von Ressourcen auf einem Host oder einer Exchange DAG, und die Ressourcengruppe kann entweder eine ganze DAG oder einzelne Datenbanken enthalten.

  Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für die in der Ressourcengruppe definierten Ressourcen gemäß dem von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

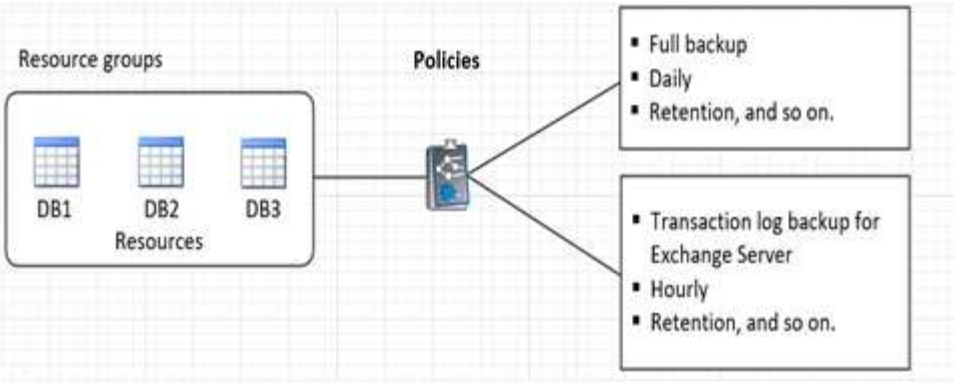
  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

  Die Ressourcengruppen wurden früher als Datensätze bezeichnet.

- Die Richtlinien legen die Backup-Häufigkeit, die Aufbewahrung von Kopien, Skripte und andere Eigenschaften von Datensicherungsvorgängen 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 ein Backup nach Bedarf für eine einzelne Ressource durchführen.

Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *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 können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass sie täglich ein vollständiges Backup durchführt, und einen anderen Zeitplan, der stündlich Protokoll-Backups durchführt. Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



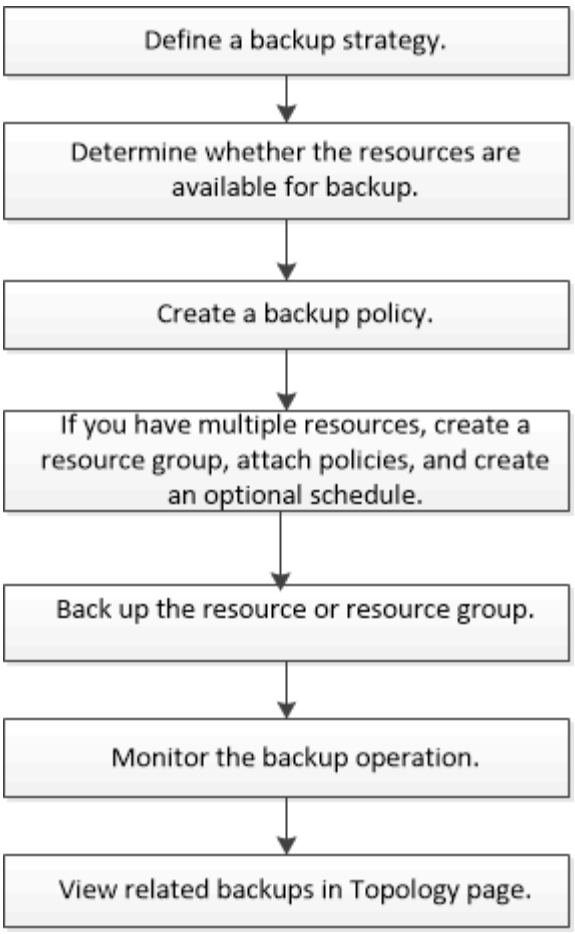
Exchange-Ressourcen sichern

Backup-Workflow

Wenn Sie das SnapCenter Plug-in für Microsoft Exchange Server in Ihrer Umgebung installieren, können Sie mit SnapCenter Exchange-Ressourcen sichern.

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden. Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden. Aktive und passive Backup-Kopien auf demselben Volume werden nicht unterstützt.

Der folgende Workflow 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 Backup-Überprüfung. Sie können jedoch das mit Exchange zur Verfügung gestellte Eseutil Tool verwenden, um Exchange-Datenbanken und Backups zu überprüfen.

Das Microsoft Exchange Eseutil Tool ist ein Befehlszeilen-Dienstprogramm, das in Ihrem Exchange Server enthalten ist. Das Dienstprogramm ermöglicht die Durchführung von Konsistenzprüfungen zur Überprüfung der Integrität von Exchange-Datenbanken und Backups.

Best Practice: Es ist nicht erforderlich, Konsistenzprüfungen auf Datenbanken durchzuführen, die Teil einer Database Availability Group (DAG) Konfiguration mit mindestens zwei Replikaten sind.

Weitere Informationen finden Sie unter "Microsoft Exchange Server-Dokumentation".

Bestimmen Sie, ob Exchange Ressourcen für Backups verfügbar sind

Ressourcen sind die Datenbanken, Exchange Database Availability Groups, die von den von Ihnen installierten Plug-ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsjobs ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie zur Verfügung haben. Das ermitteln der verfügbaren Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen, das Hinzufügen von Anmeldeinformationen und das Installieren des Plug-ins für Exchange.
- Um die Funktionen der Single Mailbox Recovery Software nutzen zu können, müssen Sie Ihre aktive Datenbank auf dem Exchange Server befinden, wo die Single Mailbox Recovery Software installiert ist.
- Wenn Datenbanken auf VMware RDM LUNs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in bei SnapCenter registrieren. Das "Dokumentation zum SnapCenter Plug-in für VMware vSphere" hat weitere Informationen.

Über diese Aufgabe

- Datenbanken können nicht gesichert werden, wenn die Option **Gesamtstatus** auf der Seite Details auf nicht verfügbar für Backups eingestellt ist. Die Option **Gesamtstatus** ist für die Sicherung auf nicht verfügbar eingestellt, wenn eine der folgenden Optionen zutrifft:
  - Datenbanken sind nicht auf einer NetApp LUN.
  - Datenbanken befinden sich nicht im normalen Zustand.

    Datenbanken befinden sich nicht im normalen Zustand, wenn sie sich im Mount-, Unmount-, erneutes Seeding oder Recovery-Wartezustand befinden.
- Wenn Sie über eine Datenbankverfügbarkeitsgruppe (DAG) verfügen, können Sie alle Datenbanken in der Gruppe sichern, indem Sie den Sicherungsauftrag von der DAG ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann in der Dropdown-Liste Plug-ins in der oberen linken Ecke der Seite Ressourcen * Microsoft Exchange Server* aus.
2. Wählen Sie auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** die Option **Datenbank**, oder **Database Availability Group** 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 Sie auf , und wählen Sie den Hostnamen und den Exchange Server aus, um die Ressourcen zu filtern. Sie können dann klicken , um den Filterbereich zu schließen.
3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden in den SnapCenter-Serverbestand 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 sich die Datenbank zurzeit befindet, Server mit Kopien, Zeitpunkt des letzten Backups und Gesamtstatus angezeigt.
   - Wenn sich die Datenbank auf einem Speicher außerhalb von NetApp befindet, wird in der Spalte Status insgesamt kein Backup verfügbar angezeigt.

     Wenn sich in einer DAG die aktive Datenbankkopie auf einem Storage anderer Anbieter befindet und

mindestens eine passive Datenbankkopie auf NetApp Storage ist, wird in der Spalte **Gesamtstatus** nicht geschützt angezeigt.

Sie können keine Datensicherungsvorgänge für eine Datenbank ausführen, die sich auf einem Storage-Typ außerhalb von NetApp befindet.

- Wenn sich die Datenbank auf NetApp Storage befindet und nicht geschützt ist, wird sie in der Spalte **Gesamtstatus** nicht geschützt angezeigt.
- Wenn sich die Datenbank auf einem NetApp Storage System befindet und geschützt ist, zeigt die Benutzeroberfläche die Meldung Backup not run in der Spalte **Gesamtstatus** an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist und das Backup für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche die Meldung Sicherung erfolgreich in der Spalte **Gesamtstatus** an.

Erstellen von Backup-Richtlinien für Exchange Server-Datenbanken

Sie können eine Backup-Richtlinie für die Exchange-Ressourcen oder für die Ressourcengruppen erstellen, bevor Sie SnapCenter zum Sichern von Microsoft Exchange Server-Ressourcen verwenden. Alternativ können Sie beim Erstellen einer Ressourcengruppen oder beim Backup einer einzelnen Ressource eine Backup-Richtlinie erstellen.

Bevor Sie beginnen

- Sie müssen Ihre Datensicherungsstrategie definiert haben.

  Weitere Informationen finden Sie in den Informationen zur Definition einer Datensicherungsstrategie für Exchange Datenbanken.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Storage-System abschließen.
- Sie müssen die Exchange Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss der SnapCenter Administrator Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.
- Wenn Sie die PowerShell-Skripte in Verordnungen und Postskripten ausführen möchten, sollten Sie den Wert des Parameters in der Datei auf true setzen `usePowershellProcessforScripts` `web.config` .

  Der Standardwert ist false.

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

Über diese Aufgabe

- Eine Backup-Richtlinie ist eine Reihe von Regeln, die festlegen, wie Backups gemanagt und aufbewahrt werden und wie oft die Ressourcen- oder Ressourcengruppe gesichert wird. Außerdem können Sie Skripteinstellungen festlegen. Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.
- Eine vollständige Backup-Aufbewahrung ist spezifisch für eine bestimmte Richtlinie. Eine Datenbank oder Ressource, die Richtlinien A mit einer vollständigen Backup-Aufbewahrung von 4 verwendet, behält 4 volle

Backups bei und hat keine Auswirkungen auf Richtlinie B für die gleiche Datenbank oder Ressource, die möglicherweise eine Aufbewahrung von 3 haben, um 3 vollständige Backups aufzubewahren.

- Die Backup-Aufbewahrung von Protokollen ist über alle Richtlinien hinweg wirksam und wird für alle Backup-Protokollierung einer Datenbank oder Ressource angewendet. Wenn ein vollständiges Backup mit Richtlinie B durchgeführt wird, wirkt sich die Einstellung für die Protokollaufbewahrung auf die von Richtlinie A erstellten Protokoll-Backups in derselben Datenbank oder Ressource aus. Ebenso wirkt sich die Einstellung für die Protokollaufbewahrung für Policy A auf die von Richtlinie B erstellten Protokoll-Backups in derselben Datenbank aus.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

  Best Practice: Es ist am besten, dass Sie die sekundäre Aufbewahrungsrichtlinie auf der Grundlage der Anzahl der vollständigen und Log-Backups insgesamt konfigurieren, die Sie behalten möchten. Wenn Sie sekundäre Aufbewahrungsrichtlinien konfigurieren, beachten Sie, dass bei Datenbanken und Protokollen, die sich auf verschiedenen Volumes befinden, jedes Backup drei Snapshots haben kann. Wenn sich Datenbanken und Protokolle auf demselben Volume befinden, kann jedes Backup zwei Snapshots haben.

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

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

    Bei ONTAP 9.12.1 und älteren Versionen übernehmen die über die SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

  Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

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 Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Sicherungstyp die folgenden Schritte durch:

   a. Wählen Sie den Sicherungstyp:

Ihr Ziel ist	Tun Sie das…
Sichern Sie die Datenbankdateien und die erforderlichen Transaktions-Logs	Wählen Sie **Vollbackup und Log Backup** aus. Datenbanken werden durch Log-Verkürzung gesichert und alle Protokolle werden gesichert, einschließlich der gekürzten Protokolle. Dies ist der empfohlene Backup-Typ.
Sichern Sie die Datenbankdateien und die nicht gesicherten Transaktionsprotokolle	Wählen Sie * Vollbackup* aus. Datenbanken werden durch Log-Verkürzung gesichert, gekürzte Protokolle werden nicht gesichert.
Sichern Sie alle Transaktions-Logs	Wählen Sie **Backup protokollieren**. Alle Transaktions-Logs auf dem aktiven File-System werden gesichert, und es gibt keine Log-Verkürzung. Ein Verzeichnis *sceBackupinfo* wird auf derselben Festplatte erstellt wie das Live Log. Dieses Verzeichnis enthält den Zeiger auf die inkrementellen Änderungen für die Exchange-Datenbank und entspricht nicht den vollständigen Log-Dateien.
Sichern Sie alle Datenbank- und Transaktions-Logs, ohne die Transaktions-Log-Dateien zu beeinträchtigen	Wählen Sie **Backup Kopieren**. Alle Datenbanken und Protokolle werden gesichert, und es gibt keine Log-Verkürzung. In der Regel verwenden Sie diesen Backup-Typ für das erneutes Seeding einer Kopie oder zum Testen oder zur Diagnose eines Problems.

Sie sollten den für die Protokoll-Backups benötigten Speicherplatz basierend auf der vollständigen Backup-Aufbewahrung definieren, nicht auf der Grundlage einer up-to-the-minute-Aufbewahrung (UTM).

Erstellen Sie beim Umgang mit Exchange Volumes (LUNs) separate Vault-Richtlinien für Protokolle und Datenbanken, und setzen Sie die Keep (Retention) für die Protokollrichtlinie auf die doppelte Anzahl für jedes Label wie die Datenbankrichtlinie unter Verwendung derselben Labels. Weitere Informationen finden Sie unter: "Bei Backups mit SnapCenter für Exchange wird nur die Hälfte der Snapshots auf dem Ziel-Log-Volume von Vault gespeichert"

b. Wählen Sie im Abschnitt Einstellungen für Datenbankverfügbarkeitsgruppen eine Aktion aus:

Für dieses Feld…	Tun Sie das…
Sichern Sie aktive Kopien	Wählen Sie diese Option aus, um nur die aktiven Kopien der ausgewählten Datenbank zu sichern. Bei Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAGs) werden mit dieser Option nur aktive Kopien aller Datenbanken in der DAG gesichert. Passive Kopien werden nicht gesichert.
Sichern Sie Kopien auf Servern, die zum Erstellungszeitpunkt des Backup-Jobs ausgewählt werden sollen	Wählen Sie diese Option aus, um alle Kopien der Datenbanken auf den ausgewählten Servern zu sichern, sowohl aktiv als auch passiv. Bei DAGs sichert diese Option sowohl aktive als auch passive Kopien aller Datenbanken auf den ausgewählten Servern.

Bei Cluster-Konfigurationen werden die Backups entsprechend den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Node des Clusters aufbewahrt. Wenn sich der Owner-Node des Clusters ändert, werden die Backups des vorherigen Owner-Node beibehalten. Die Aufbewahrung gilt nur auf Node-Ebene.

c. Wählen Sie im Abschnitt Terminfrequenz einen oder mehrere der Frequenztypen aus: **On Demand**, **hourly**, **Daily**, **Weekly** und **Monthly**.

Sie können den Zeitplan (Startdatum, Enddatum) für Sicherungsvorgänge beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

6. Konfigurieren Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen.

   Die angezeigten Optionen hängen vom Backup-Typ und vom Frequenztyp ab, den Sie zuvor ausgewählt haben.

Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.

Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

a. Wählen Sie im Abschnitt Einstellungen für die Aufbewahrung von Protokollsicherungen eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Bewahren Sie nur eine bestimmte Anzahl von Protokoll-Backups auf	Wählen Sie **Anzahl der vollständigen Backups, für die Protokolle aufbewahrt werden**, und geben Sie die Anzahl der vollständigen Backups an, für die Sie eine zeitnahe Wiederherstellung wünschen. Die up-to-the-minute (UTM) Aufbewahrung gilt für die Protokollierung der Backups, die über vollständige Backups oder das Log-Backup erstellt wurden. Wenn die UTM-Aufbewahrungseinstellungen beispielsweise so konfiguriert sind, dass die Protokollsicherungen der letzten 5 vollständigen Backups gespeichert werden, werden die Protokoll-Backups der letzten 5 vollständigen Backups beibehalten. Die im Rahmen der vollständigen und der Log-Backups erstellten Protokollordner werden automatisch als Teil von UTM gelöscht. Sie können die Protokollordner nicht manuell löschen. Wenn z. B. die Aufbewahrungseinstellung für vollständige oder vollständige Backup und Log-Sicherung für einen Monat festgelegt ist und die UTM-Aufbewahrung auf 10 Tage festgelegt ist, wird der im Rahmen dieser Backups erstellte Log-Ordner wie pro UTM gelöscht. Dadurch sind nur 10 Tage Protokollordner vorhanden und alle anderen Backups sind für die Point-in-Time-Wiederherstellung markiert. Sie können den UTM-Aufbewahrungswert auf 0 einstellen, wenn Sie keine minutengenaue Wiederherstellung durchführen möchten. Dies ermöglicht den Point-in-Time Restore-Vorgang. **Best Practice:** Es ist am besten, dass die Einstellung gleich der Einstellung für Total Snapshots (Full Backups) im Abschnitt Full Backup Retention Settings sein muss. Dadurch wird sichergestellt, dass Protokolldateien für jedes vollständige Backup aufbewahrt werden.

Ihr Ziel ist	Tun Sie das…
Bewahren Sie die Backup-Kopien für eine bestimmte Anzahl von Tagen auf	Wählen Sie die Option **Protokollsicherungen für letzte** aufbewahren und geben Sie die Anzahl der Tage an, um die Backup-Kopien des Protokolls zu behalten. Aufbewahrung der Log-Backups bis zur Anzahl von Tagen voller Backups.
Sperrfrist von Snapshots	Wählen Sie **Sperrfrist der Snapshot-Kopie** aus und wählen Sie Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

Wenn Sie als Backup-Typ **Log Backup** ausgewählt haben, werden Log-Backups als Teil der up-to-the-minute-Aufbewahrungseinstellungen für vollständige Backups beibehalten.

b. Wählen Sie im Abschnitt Einstellungen für vollständige Backups eine der folgenden Optionen für On-Demand-Backups aus, und wählen Sie dann eine für vollständige Backups aus:

Für dieses Feld…	Tun Sie das…
Bewahren Sie nur eine bestimmte Anzahl von Snapshots auf	Wenn Sie die Anzahl der vollständigen Backups angeben möchten, die beibehalten werden sollen, wählen Sie die Option **Total Snapshot Copies to keep** aus, und geben Sie die Anzahl der Snapshots (Full Backups) an, die beibehalten werden sollen. Wenn die Anzahl der vollständigen Backups die angegebene Anzahl überschreitet, werden die vollständigen Backups, die die angegebene Anzahl überschreiten, gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.
Bewahren Sie vollständige Backups für eine bestimmte Anzahl an Tagen auf	Wählen Sie die Option **Snapshot Kopien behalten für** und geben Sie die Anzahl der Tage an, die Snapshots behalten werden sollen (vollständige Backups).
Sperrfrist von Snapshots	Wählen Sie **Sperrfrist der Snapshot-Kopie** aus und wählen Sie Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

Wenn Sie eine Datenbank mit nur Protokollsicherungen und keinen vollständigen Backups auf einem Host in einer DAG-Konfiguration haben, werden die Protokoll-Backups auf folgende Weise beibehalten:

- Standardmäßig findet SnapCenter auf allen anderen Hosts in der DAG das älteste volle Backup

dieser Datenbank und löscht alle Log-Backups auf diesem Host, die vor dem vollständigen Backup erstellt wurden.

- Sie können das oben genannte Standard-Aufbewahrungsverhalten für eine Datenbank auf einem Host in einer DAG mit nur Protokoll-Backups überschreiben, indem Sie den Schlüssel **MaxLogBackupOnlyCountWithfullBackup** in der Datei *C:\Programme\NetApp\SnapCenter WebApp\Web.config* hinzufügen.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

Im Beispiel bedeutet der Wert 10, dass Sie bis zu 10 Log-Backups auf dem Host aufbewahren.

7. Wählen Sie auf der Seite Replikation eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu behalten. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Diese Option sollte für SnapMirror Active Sync aktiviert sein. Die nur-Primärrichtlinie 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. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Siehe "Zeigen Sie Exchange-Backups auf der Seite Topologie an".
Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.

Für dieses Feld…	Tun Sie das…
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

8. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Backup ausgeführt werden sollen.
   - Zu den vorkript-Backup-Argumenten gehören „` USD Datenbank`“ und „` USD ServerInstance`“.
   - Zu den PostScript-Backup-Argumenten gehören „` USD Datenbank`“, „` USD ServerInstance`“, „` USD BackupName`“, „` USD LogDirectory`“ und „` USD LogSnapshot`“.

     Sie können ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

     Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Exchange-Server

Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des zu erfütienden Datenschutzauftrags und den Schutzzeitplan zu definieren.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

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

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.

Für dieses Feld…	Tun Sie das…
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: *Custext_resourcegruppe_Policy_hostname* oder *resourcegruppe_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite Ressourcen die folgenden Schritte aus:
   a. Wählen Sie in den Dropdown-Listen den Ressourcentyp und die Datenbankverfügbarkeitsgruppe aus, um die Liste der verfügbaren Ressourcen zu filtern.

      Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

      In den Abschnitten Verfügbare Ressourcen und ausgewählte Ressourcen wird der Datenbankname mit dem FQDN des Hosts angezeigt. Dieser FQDN gibt nur an, dass die Datenbank auf diesem spezifischen Host aktiv ist und möglicherweise keine Sicherungskopie auf diesem Host erstellt. Wählen Sie einen oder mehrere Backup-Server aus der Serverauswahl aus, wo Sie eine Sicherung erstellen möchten, falls Sie in der Richtlinie die Option **Sicherungskopien auf Servern ausgewählt haben, die bei der Erstellung von Sicherungsjobs** ausgewählt werden sollen.

   b. Geben Sie den Namen der Ressource in das Suchfeld ein, oder scrollen Sie, um nach einer Ressource zu suchen.
   c. Führen Sie einen der folgenden Schritte aus, um Ressourcen aus dem Abschnitt Verfügbare Ressourcen in den Abschnitt Ausgewählte Ressourcen zu verschieben:
      - Wählen Sie **Automatische Auswahl aller Ressourcen auf demselben Speichervolumen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
      - Wählen Sie im Abschnitt „Verfügbare Ressourcen“ die Ressourcen aus, und klicken Sie dann auf den Pfeil nach rechts, um sie in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.

        Ressourcengruppen von SnapCenter für Microsoft Exchange Server dürfen nicht mehr als 30 Datenbanken pro Snapshot enthalten. Wenn mehr als 30 Datenbanken in einer Ressourcengruppe vorhanden sind, wird ein zweiter Snapshot für die zusätzlichen Datenbanken erstellt. Deshalb werden 2 Unterjobs unter dem Hauptsicherungsjob erzeugt. Für Backups mit sekundärer Replikation, während SnapMirror oder SnapVault Update läuft, kann es Szenarien geben, in denen sich das Update für die beiden Unterjobs überlappen. Der wichtigste Backup-Job läuft dauerhaft, auch wenn die Protokolle darauf hindeuten, dass der Job abgeschlossen ist.

6. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

Wenn eine Richtlinie die Option **Sicherungskopien auf Servern enthält, die bei der Erstellung von Sicherungsjobs** ausgewählt werden sollen, wird eine Serverauswahloption angezeigt, die einen oder mehrere Server auswählt. Die Serverauswahl-Option listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf dem NetApp Storage befindet.

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

b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies auf * + **in der Spalte *Configure Schedules** für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

c. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **OK** klicken.

Sie müssen dies für jede in der Richtlinie angegebene Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte **angewendete Zeitpläne** im Abschnitt Zeitpläne für ausgewählte Richtlinien konfigurieren aufgelistet.

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

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

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

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

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

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

Erstellen Sie eine Storage-Systemverbindung und Zugangsdaten mit PowerShell cmdlets für Exchange Server

Bevor Sie PowerShell cmdlets verwenden können, müssen Sie eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, um ein Backup und eine Wiederherstellung durchzuführen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt

werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mit dem `Open-SmConnection` Cmdlet.

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

   ```
   PS C:\> Open-SmConnection
   ```

2. Erstellen Sie mit dem Cmdlet eine neue Verbindung zum Speichersystem `Add-SmStorageConnection` .

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Erstellen Sie mit dem Cmdlet ein neues Run As-Konto `Add-Credential` .

   In diesem Beispiel wird ein neuer Lauf als Konto mit dem Namen ExchangeAdmin mit Windows-Anmeldeinformationen erstellt:

   ```
   PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

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

Backup von 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 Aggregat, das vom Backup-Vorgang verwendet wird, der SVM zugewiesen haben, die von der Datenbank verwendet wird.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern

möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

- Wenn Sie ein Backup einer Datenbank oder einer Database Availability Group durchführen möchten, die über eine aktiv/Passiv-Datenbankkopie auf NetApp Storage und Storage anderer Anbieter verfügt, Und Sie haben **aktive Kopien sichern** oder **Sicherungskopien auf Servern ausgewählt, die während der Erstellung von Sicherungsaufträgen ausgewählt werden sollen** Option in der Richtlinie wird der Sicherungsauftrag in den Warnstatus versetzt. Das Backup führt erfolgreich eine aktive/passive Datenbankkopie auf NetApp Storage durch und ein Backup schlägt fehl bei der aktiv/passiven Datenbankkopie auf Storage anderer Anbieter.

  Best Practice: führen Sie keine Backups aktiver und passiver Datenbanken gleichzeitig aus. Es kann zu einem Wettlauf kommen, und eine der Sicherungen schlägt möglicherweise fehl.

UI von SnapCenter

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 **Datenbank-Verfügbarkeitsgruppe** aus der Liste **Ansicht** aus.

   Auf der Seite „Ressourcen“ gibt das  Symbol an, dass sich die Datenbank auf Storage anderer Anbieter befindet.

   Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Storage anderer Anbieter befindet und mindestens eine passive Datenbankkopie auf einem NetApp Storage gespeichert ist, 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 – Ressourcen 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: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den 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 Dropdown-Liste aus.

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

      Wenn eine Richtlinie die Option **Sicherungskopien auf Servern enthält, die bei der Erstellung von Sicherungsjobs** ausgewählt werden sollen, wird eine Serverauswahloption angezeigt, die einen oder mehrere Server auswählt. Die Serverauswahl-Option listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf einem NetApp Storage befindet.

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

   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf * * für die Richtlinie, für die Sie einen

Zeitplan konfigurieren möchten.

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

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

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

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

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

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

Die Seite der Datenbanktopologie wird angezeigt.

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

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

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

b. Klicken Sie Auf **Backup**.

9. Überwachen Sie den Fortschritt des Backups, indem Sie im Aktivitätsbereich unten auf der Seite auf den Job doppelklicken, um die Seite „Jobdetails“ anzuzeigen.

- In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der 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 auf Folgendes: *Java -jar -Xmx8192M -Xms4096M*

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   In diesem Beispiel wird eine neue Backup-Richtlinie mit einem vollständigen Exchange Backup-Typ für Backups und Protokollierung erstellt:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

   Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem stündlichen vollständigen Backup und Log Backup-Typ für Exchange Backup:

```
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 Backup-Richtlinie erstellt, in der nur Exchange-Protokolle gesichert werden:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Ermitteln Sie Host-Ressourcen mit dem Cmdlet "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 mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter hinzu.

   In diesem Beispiel wird eine neue Backup-Ressourcengruppe für die Exchange Server-Datenbank 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_Lo
g_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'}
```

Dieses Beispiel erstellt eine neue Exchange Database Availability Group (DAG) Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

```
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_Lo
g_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

Dieses Beispiel erstellt ein neues Backup im Sekundärspeicher:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

In diesem Beispiel wird ein Job-Summary-Bericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Dieses Beispiel zeigt einen Job-Übersichtsbericht für eine bestimmte Job-ID an:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ siehe

"SnapCenter Software Cmdlet Referenzhandbuch".

Sichern von Exchange-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG, und die Ressourcengruppe kann entweder eine vollständige DAG oder individuelle Datenbanken enthalten. Sie können die Ressourcengruppen auf der Seite Ressourcen sichern.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Sie müssen das Aggregat, das vom Backup-Vorgang verwendet wird, der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts enthält, kann der Backup-Vorgang bei einigen Hosts aufgrund von Netzwerkproblemen zu spät beginnen. Sie sollten den Wert von in mit dem PowerShell Cmdlet konfigurieren `MaxRetryForUninitializedHosts` `web.config` `Set-SmConfigSettings` .
- Wenn Sie in einer Ressourcengruppe eine Datenbank- oder Database Availability Group mit aktiver/passiver Datenbankkopie auf einem NetApp Storage und nicht-NetApp Storage einschließen, und Sie haben **aktive Kopien sichern** oder **Sichern von Kopien auf Servern ausgewählt, die während der Erstellung von Sicherungsjobs ausgewählt werden sollen**-Option in der Richtlinie, Dann werden die Sicherungsjobs in den Warnstatus gehen.

  Das Backup führt erfolgreich eine aktive/passive Datenbankkopie auf NetApp Storage durch und ein Backup schlägt fehl bei der aktiv/passiven Datenbankkopie auf Storage anderer Anbieter.

Über diese Aufgabe

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups 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 **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf * * klicken und dann das Tag auswählen. 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der

Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

b. Klicken Sie Auf **Backup**.

5. Überwachen Sie den Fortschritt des Backups, indem Sie im Aktivitätsbereich unten auf der Seite auf den Job doppelklicken, um die Seite „Jobdetails“ anzuzeigen.

Monitoring von Backup-Vorgängen

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

Überwachen Sie die Vorgänge im Teilfenster „Aktivität“

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

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

Schritte

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

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

Abbrechen der Backup-Vorgänge für die Exchange-Datenbank

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.

Von der…	Aktion
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *  , um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Zeigen Sie Exchange-Backups auf der Seite Topologie an

Wenn Sie die Datensicherung vorbereiten, ist es Ihnen eventuell hilfreich, eine grafische Darstellung aller Backups auf den primären und sekundären Speichern anzuzeigen.

Über diese Aufgabe

Auf der Seite Topology sehen Sie alle Backups, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details zu diesen Backups anzeigen und sie zur Durchführung von Datensicherungsvorgängen auswählen.

Mithilfe des folgenden Symbols in der Ansicht Kopien verwalten können Sie bestimmen, ob die Backups auf dem primären oder sekundären Speicher verfügbar sind (gespiegelte Kopien oder Vault-Kopien).

-  Zeigt die Anzahl der Backups an, die auf dem primären Speicher verfügbar sind.
-  Zeigt die Anzahl der Backups an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.
-  Zeigt die Anzahl der Backups an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.
    - Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden.

      Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Best Practice: um sicherzustellen, dass die korrekte Anzahl replizierter Backups angezeigt wird, empfehlen wir, die Topologie zu aktualisieren.

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

-

 Der Replikatstandort ist hochgefahren.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Datenbank, die Ressource oder die Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Datenbank-Detailansicht oder in der Ansicht Ressourcengruppen-Details aus.

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

4. Lesen Sie den Abschnitt „Übersichtskarte“, um eine Zusammenfassung der Anzahl der Backups anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

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

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

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

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

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

   - Bei aktiver SnapMirror Synchronisierung und nur für ONTAP 9.14.1 sollten die Beziehungen zwischen Async Mirror und Async MirrorVault zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault automatisch auf das neue primäre Ziel konfiguriert.nach dem Failover.
   - Nach dem Failover sollte ein Backup erstellt werden, damit SnapCenter den Failover erkennt. Sie können erst dann auf **Refresh** klicken, wenn ein Backup erstellt wurde.
5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** auf dem primären oder sekundären Speicher, um Details zu einem Backup anzuzeigen.

   Die Details der Backups werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um

Vorgänge zum Wiederherstellen, Umbenennen und Löschen durchzuführen.

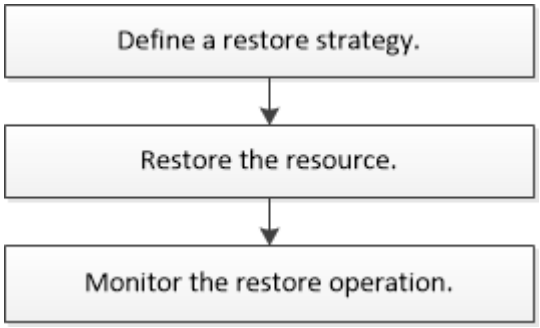
Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen. Das Löschen von Snapshots wird von den ONTAP-Aufbewahrungseinstellungen übernommen.

Stellen Sie Exchange Ressourcen wieder her

Wiederherstellung des Workflows

Mit SnapCenter können Exchange-Datenbanken wiederhergestellt werden, indem ein oder mehrere Backups auf dem aktiven File-System wiederhergestellt werden.

Im folgenden Workflow wird die Reihenfolge angezeigt, in der Sie die Wiederherstellungsvorgänge der Exchange-Datenbank durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup- und Restore-Vorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder unter "SnapCenter Software Cmdlet Referenzhandbuch".

Anforderungen 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 SnapCenter Server als auch das SnapCenter Plug-in für die Exchange-Datenbank auf 4.6 aktualisieren.

- Der Exchange Server muss online sein und ausgeführt werden, bevor Sie eine Datenbank wiederherstellen können.
- Die Datenbanken müssen auf dem Exchange Server vorhanden sein.

  Die Wiederherstellung gelöschter Datenbanken wird nicht unterstützt.

- SnapCenter-Zeitpläne für die Datenbank müssen ausgesetzt werden.
- Der SnapCenter Server und das SnapCenter Plug-in für Microsoft Exchange Server Host müssen mit dem primären und sekundären Storage verbunden sein, der die wiederherzustellenden Backups enthält.

Exchange Datenbanken wiederherstellen

Mit SnapCenter können Sie gesicherte Exchange Datenbanken wiederherstellen.

Bevor Sie beginnen

- Sie müssen die Ressourcengruppen, die Datenbank oder die Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAGs) gesichert haben.
- Wenn die Exchange-Datenbank zu einem anderen Speicherort migriert wird, funktioniert der Wiederherstellungsvorgang nicht für alte Backups.
- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.
- Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Storage anderer Anbieter befindet und Sie die passive Datenbankkopie eines Backups in einem NetApp Storage wiederherstellen möchten, erstellen Sie in einer DAG die passive Kopie (NetApp Storage) als aktive Kopie, aktualisieren Sie die Ressourcen und führen Sie den Wiederherstellungsvorgang aus.

  Führen Sie den Befehl aus `Move-ActiveMailboxDatabase` , um die passive Datenbankkopie als aktive Datenbankkopie zu erstellen.

  Das "Microsoft-Dokumentation" enthält Informationen zu diesem Befehl.

Über diese Aufgabe

- Wenn ein Restore-Vorgang für eine Datenbank durchgeführt wird, wird die Datenbank wieder auf demselben Host gemountet und es wird kein neues Volume erstellt.
- DAG-Backups müssen aus einzelnen Datenbanken wiederhergestellt werden.
- Die vollständige Wiederherstellung der Festplatte wird nicht unterstützt, wenn andere Dateien als die Exchange-Datenbank (.edb)-Datei vorhanden sind.

  Plug-in für Exchange führt keine vollständige Wiederherstellung auf einer Festplatte durch, wenn das Laufwerk Exchange-Dateien wie die zur Replizierung verwendeten enthält. Wenn eine vollständige Wiederherstellung möglicherweise die Exchange-Funktionalität beeinträchtigt, führt das Plug-in für Exchange einen Wiederherstellungsvorgang für eine einzelne Datei durch.

- Das Plug-in für Exchange kann BitLocker-verschlüsselte Laufwerke nicht wiederherstellen.
- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.

UI von SnapCenter

Schritte

1. Klicken Sie im linken Navigationsbereich oben links auf der Seite Ressource 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 Manage Copies die Option **Backups** aus der Tabelle Primary Backups aus, und klicken Sie dann auf * *  .
6. Wählen Sie auf der Seite Optionen eine der folgenden Backup-Optionen für Protokolle aus:

Option	Beschreibung
Alle Log-Backups	Wählen Sie * Alle Log-Backups*, um eine Backup-Wiederherstellung durchzuführen, um alle verfügbaren Log-Backups nach der vollständigen Sicherung wiederherzustellen.
Durch Backups bis protokollieren	Wählen Sie **by log Backups bis**, um einen Point-in-Time-Wiederherstellungsvorgang durchzuführen, der die Datenbank basierend auf Protokollsicherungen bis zum ausgewählten Protokoll wiederherstellt. Die Anzahl der in der Dropdown-Liste angezeigten Protokolle basiert auf UTM. Wenn beispielsweise die vollständige Backup-Aufbewahrung 5 ist und die UTM-Aufbewahrung 3 ist, sind die Anzahl der verfügbaren Log-Backups 5, aber im Drop-down-Menü werden nur 3 Protokolle aufgeführt, um den Wiederherstellungsvorgang durchzuführen.
Nach einem bestimmten Datum bis	Wählen Sie **nach einem bestimmten Datum bis**, um das Datum und die Uhrzeit anzugeben, auf die Transaktionsprotokolle auf die wiederhergestellte Datenbank angewendet werden. Mit diesem Point-in-Time-Wiederherstellungsvorgang werden die Transaktions-Log-Einträge wiederhergestellt, die bis zum letzten Backup am angegebenen Datum und Uhrzeit aufgezeichnet wurden.

Option	Beschreibung
Keine	Wählen Sie **Keine**, wenn Sie nur die vollständige Sicherung ohne Log-Backups wiederherstellen müssen.

Sie können eine der folgenden Aktionen durchführen:

- **Datenbank wiederherstellen und mounten nach der Wiederherstellung** - Diese Option ist standardmäßig ausgewählt.
- **Die Integrität der Transaktionsprotokolle im Backup vor der Wiederherstellung nicht überprüfen** - standardmäßig überprüft SnapCenter die Integrität der Transaktionsprotokolle in einem Backup, bevor ein Restore durchgeführt wird.

  Best Practice: Du solltest diese Option nicht wählen.

7. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Wiederherstellungsvorgang ausgeführt werden sollen.

   Prescript-Argumente für die Wiederherstellung umfassen Datenbanken in US-Dollar und ServerInstance in US-Dollar.

   Zu den Argumenten für die Wiederherstellung nach dem Skript gehören Datenbanken in US-Dollar, ServerInstance, Backup-Name in US-Dollar, LogDirectory und TargetServerInstance in US-Dollar.

   Sie können ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren, Protokolle zu senden usw.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

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

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

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Sie können den Status des Wiederherstellungsjobs anzeigen, indem Sie unten auf der Seite das Feld „Aktivität“ erweitern.

    Sie sollten den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs** überwachen.

Wenn Sie eine aktive Datenbank aus einem Backup wiederherstellen, weist die passive Datenbank möglicherweise einen Status „ausgesetzt“ oder „ausgefallen“ auf, wenn eine Verzögerung zwischen dem Replikat und der aktiven Datenbank vorhanden ist.

Die Statusänderung kann auftreten, wenn die Protokollkette der aktiven Datenbank sich gabelt und einen neuen Zweig startet, der die Replikation unterbrochen. Exchange Server versucht, das Replikat zu reparieren. Wenn es jedoch nicht möglich ist, sollten Sie nach der Wiederherstellung ein neues Backup erstellen und dann das Replikat erneut übertragen.

PowerShell Commandlets

Schritte

1. Starten Sie mit dem Cmdlet eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer `Open-SmConnection` .

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

2. Rufen Sie mit dem Cmdlet die Informationen über ein oder mehrere Backups ab, die Sie wiederherstellen möchten `Get-SmBackup` .

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 dem Backup mit dem Cmdlet wieder `Restore-SmBackup` her.

   In diesem Beispiel wird ein minutengenaue Backup 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 ein zeitpunktgenaues Backup 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 ein Backup auf sekundärem Storage auf einen primären Erfahrungsbericht wiederhergestellt:

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BackupId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

Mit dem `-archive` Parameter können Sie die primären und sekundären Volumes angeben, die Sie für die Wiederherstellung verwenden möchten.

Mit dem `-IsRecoverMount:$true` Parameter können Sie die Datenbank nach der Wiederherstellung mounten.

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

Granulares Recovery von Mails und Mailboxen

Die Single Mailbox Recovery Software (SMBR) ermöglicht es Ihnen, Mails oder Postfächer anstelle der gesamten Exchange Datenbank wiederherzustellen.

Das Wiederherstellen einer vollständigen Datenbank für die Wiederherstellung einer einzelnen Mail benötigt viel Zeit und Ressourcen. SMBR hilft bei der schnellen Wiederherstellung der Mails durch die Erstellung von Klonkopien des Snapshots und dann mit Microsoft APIs, um die Mailbox in SMBR zu mounten. Informationen zur Verwendung von SMBR finden Sie unter "SMBR-Administrationshandbuch".

Weitere Informationen zu SMBR finden Sie nachfolgend:

- "Anleitung zur manuellen Wiederherstellung eines einzelnen Elements mit SMBR (gilt auch für Wiederherstellungen bei Ontrack Power Control)"
- "Wiederherstellung aus dem sekundären Storage in SMBR mit SnapCenter"
- "Wiederherstellung von Microsoft Exchange Mail über SnapVault mit SMBR"

Wiederherstellung einer Exchange Server-Datenbank aus dem sekundären Storage

Sie können eine gesicherte Exchange Server Datenbank aus dem sekundären Storage (Spiegel oder Vault) wiederherstellen.

Sie müssen die Snapshots vom primären Speicher auf einen sekundären Speicher repliziert haben.

Über diese Aufgabe

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **Microsoft Exchange Server Plug-in** aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** die Option **Datenbank** oder **Ressourcengruppe** aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus.

   Die Topologieseite für die Datenbank- oder Ressourcengruppe wird angezeigt.
4. Wählen Sie im Abschnitt Kopien verwalten aus dem sekundären Speichersystem (Spiegel oder Tresor) **Backups** aus.
5. Wählen Sie das Backup aus der Liste aus, und klicken Sie dann auf  .
6. Wählen Sie auf der Seite Standort das Zielvolume für die Wiederherstellung der ausgewählten Ressource aus.
7. Schließen Sie den Wiederherstellungs-Assistenten ab, überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erneutes Seeding eines passiven Exchange Node-Replikats

Wenn Sie eine Replikatkopie erneut übertragen müssen, beispielsweise wenn eine Kopie beschädigt ist, können Sie sie mithilfe der Funktion zum erneuten Seeding in SnapCenter erneut in das neueste Backup übertragen.

Bevor Sie beginnen

- Sie müssen SnapCenter Server 4.1 oder höher und Plug-in für Exchange 4.1 oder höher verwenden.

  Erneutes Seeding eines Replikats wird in SnapCenter-Versionen vor 4.1 nicht unterstützt.
- Sie müssen eine Sicherung der Datenbank erstellt haben, die Sie erneut senden möchten.

Best Practice: um einen Rückgang zwischen den Knoten zu vermeiden, empfehlen wir Ihnen, entweder ein neues Backup zu erstellen, bevor Sie einen erneuten Vorgang durchführen, oder den Host mit dem neuesten Backup auszuwählen.

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 Ansicht aus:

Option	Beschreibung
Zum erneuten Seeding einer einzelnen Datenbank	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Zum erneuten Seeding von Datenbanken in einer DAG	Wählen Sie in der Liste View die Option **Database Availability Group** aus.

3. Wählen Sie die Ressource aus, die erneut gesendet werden soll.

4. Klicken Sie auf der Seite Kopien verwalten auf **erneut**.
5. Wählen Sie aus der Liste der ungesunden Datenbankkopien im Assistenten zum erneuten Seeding den aus, den Sie erneut speichern möchten, und klicken Sie dann auf **Weiter**.
6. Wählen Sie im Host-Fenster den Host mit dem Backup aus, von dem Sie erneut starten möchten, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

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

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
9. Sie können den Status des Jobs anzeigen, indem Sie das Aktivitätsfenster unten auf der Seite erweitern.

Ein erneutes Seeding wird nicht unterstützt, wenn die passive Datenbankkopie auf Storage anderer Anbieter liegt.

Erneutes Seeding mit PowerShell cmdlets für Exchange Datenbank

Sie können PowerShell Cmdlets verwenden, um eine fehlerhafte Kopie wiederherzustellen, indem Sie entweder die aktuellste Kopie auf demselben Host oder die aktuellste Kopie von einem alternativen Host verwenden.

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

Schritte

1. Starten Sie mit dem Cmdlet eine Verbindungssitzung mit dem SnapCenter-Server für einen angegebenen Benutzer `Open-SmConnection` .

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Erneutes Seeding der Datenbank mit dem `reseed-SmDagReplicaCopy` Cmdlet.

   In diesem Beispiel wird die fehlgeschlagene Kopie der Datenbank namens execdb auf dem Host „mva-rx200.netapp.com" unter Verwendung des neuesten Backups auf diesem Host erneut bereitgestellt.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   In diesem Beispiel wird die fehlgeschlagene Kopie der Datenbank namens execdb erneut mit dem neuesten Backup der Datenbank (Produktion/Kopie) auf einem alternativen Host „mva-rx201.netapp.com.""“ neu definiert

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

Überwachen von Restore-Vorgängen

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

Über diese Aufgabe

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

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

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

Schritte

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

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

Abbrechen von Wiederherstellungsvorgängen für Exchange-Datenbank

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

Sie sollten als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Nachdem Sie den Wiederherstellungsvorgang gestartet haben, klicken Sie auf das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Schutz von IBM DB2

SnapCenter Plug-in für IBM DB2

Übersicht über das SnapCenter Plug-in für IBM DB2

Das SnapCenter Plug-in für IBM DB2 Database ist eine Host-seitige Komponente der NetApp SnapCenter Software, die ein applikationsspezifisches Datensicherungsmanagement von IBM DB2 Datenbanken ermöglicht. Das Plug-in für IBM DB2 Database automatisiert das Backup, die Wiederherstellung und das Klonen von IBM DB2-Datenbanken in einer 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 wird zudem IBM DB2 auf AIX unterstützt.

SnapCenter unterstützt DB2-Setups mit einer und mehreren Instanzen. Sie können das Plug-in für IBM DB2 Database sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird DB2 als manuelle Ressource unterstützt.

DB2 pureScale-Umgebung und DB2 Multi Node (DPF)-Systeme werden nicht unterstützt.

Bei der Installation des Plug-in für IBM DB2 Database können Sie SnapCenter mit NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Mithilfe des Plug-ins in mit NetApp SnapVault Technologie lässt sich darüber hinaus eine Disk-to-Disk-Backup-Replizierung zur Einhaltung von Standards durchführen.

Das SnapCenter Plug-in für DB2 unterstützt NFS und SAN unter File-Storage-Layouts von ONTAP und Azure NetApp.

VMDK oder virtuelles Storage Layout wird nicht unterstützt.

Was Sie mit dem SnapCenter-Plug-in für IBM DB2 tun können

Wenn Sie das Plug-in für IBM DB2 Database in Ihrer Umgebung installieren, können Sie mit SnapCenter IBM DB2-Datenbanken und deren Ressourcen sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Hinzufügen von Datenbanken:
- Backups erstellen.
- Restore aus Backups:
- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

Funktionen des SnapCenter Plug-ins für IBM DB2

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Um mit dem Plug-in für 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. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore- und Klonvorgänge über alle Plug-ins hinweg, die zentralisierte Berichterstellung, die Schnellübersicht über Dashboard-Ansichten, die Einrichtung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Jobs in allen Plug-ins.

- **Automatisierte zentrale Verwaltung**

  Sie können Backup-Vorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Technologie für unterbrechungsfreie NetApp Snapshot Kopien**

  SnapCenter verwendet NetApp Snapshot-Technologie mit dem Plug-in für IBM DB2 Database, um Ressourcen zu sichern.

Die Verwendung des Plug-ins für IBM DB2 bietet zudem folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktgenauer Kopien von Ressourcen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Unterstützung der Snapshot-Funktion von ONTAP für Konsistenzgruppe (CG) beim Erstellen von Backups.
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Fähigkeit, Snapshots mit externen Befehlen zu erstellen.
- Unterstützung für Linux LVM auf XFS-Dateisystem.

Vom SnapCenter-Plug-in für IBM DB2 unterstützte Storage-Typen

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines (VMs). Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter-Plug-in für IBM DB2 installieren.

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datastores • VMDKs auf VMFS erstellt • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Für das IBM DB2-Plug-in sind minimale ONTAP-Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun erstellen
  - lun erstellen
  - lun erstellen
  - lun löschen

- lun Initiatorgruppe hinzufügen
- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen

    - Show-Disk-Nutzung für Volume-Dateien
    - Volume ist offline
    - Das Volume ist online
    - Volume-Änderung
    - Erstellen von Volume-qtree
    - Volume qtree löschen
    - Änderung des Volume-qtree
    - Volume-qtree anzeigen
    - Volume-Einschränkung
    - Volumen anzeigen
    - Erstellen von Volume-Snapshots
    - Volume Snapshot löschen
    - Ändern des Volume-Snapshots
    - Volume Snapshot modify-snaplock-expiry-time
    - Umbenennung von Volume-Snapshots
    - Wiederherstellung von Volume Snapshots
    - Restore-Datei für Volume Snapshots
    - Volume-Snapshot werden angezeigt
    - Volume-Aufhängung nicht verfügbar
    - cifs von vserver
    - erstellung von cifs-Freigaben von vserver
    - cifs-Freigabe von vserver: Löschen
    - vserver cifs shadowcopy anzeigen
    - cifs-Freigabe von vserver wird angezeigt
    - vserver cifs zeigen
    - vserver Exportrichtlinie
    - Erstellung von vserver Exportrichtlinien
    - vserver: Löschen der Exportrichtlinie
    - Erstellung von vserver Export-Policy-Regel
    - vserver: Export-Policy-Regel anzeigen
    - vserver Export-Policy wird angezeigt
    - vserver iscsi
    - vserver iscsi-Verbindung wird angezeigt
    - vserver zeigen
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle
    - Netzwerkschnittstelle wird angezeigt

- vserver

Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replizierung für IBM DB2 vor

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie für IBM DB2

Definieren Sie eine Backup-Strategie für IBM DB2

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre Ressourcen erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Über diese Aufgabe

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.
2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Entscheiden Sie, ob Sie eine Richtlinie für auf Snapshot Kopien basierende erstellen möchten, um applikationskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
6. Legen Sie den Aufbewahrungszeitraum für die Snapshots auf dem Quell-Storage-System und dem SnapMirror Ziel fest.
7. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Automatische Ermittlung von Ressourcen auf Linux-Host

Ressourcen sind IBM DB2-Datenbanken und Instanzen auf dem Linux-Host, die von SnapCenter gemanagt 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.

Art der unterstützten Backups

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot Kopien basierenden Backup-Typ für IBM DB2-Datenbanken.

Backup auf Basis von Snapshot Kopien

Auf Snapshot-Kopien basierende Backups nutzen die NetApp Snapshot-Technologie, um Online-schreibgeschützte Kopien der Volumes zu erstellen, auf denen sich die IBM DB2-Datenbanken befinden.

So verwendet das SnapCenter-Plug-in für IBM DB2 Snapshots von Konsistenzgruppen

Sie können das Plug-in verwenden, um Snapshots von Konsistenzgruppen für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes beherbergen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe ist simultane Snapshots mehrerer Volumes und stellt konsistente Kopien einer Gruppe von Volumes bereit.

Sie können auch die Wartezeit für den Speicher-Controller angeben, um Snapshots konsistent zu gruppieren. Die verfügbaren Optionen für Wartezeiten sind **dringend**, **Medium** und **entspannt**. Sie können auch die WAFL-Synchronisierung (Write Anywhere File Layout) während eines konsistenten Gruppen-Snapshots aktivieren oder deaktivieren. WAFL Sync verbessert die Performance eines Consistency Group Snapshots.

So managt SnapCenter die Organisation von Daten-Backups

SnapCenter managt die Durchführung von Daten-Backups auf der Storage-System- und File-System-Ebene.

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 Backup-Zeitplänen für IBM DB2

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, die Service Level Agreement (SLA) und den Recovery Point Objective (RPO).

Backup-Zeitpläne haben zwei Teile:

- Backup-Häufigkeit (Häufigkeit der Durchführung von Backups)

  Die Backup-Häufigkeit, die auch als Zeitplantyp für einige Plug-ins bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau dann, wenn Backups durchgeführt werden)

  Backup-Zeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird

Anzahl der für IBM DB2 erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Backup-Namenskonventionen für Plug-in für IBM DB2-Datenbanken

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Restore- und Recovery-Strategie für IBM DB2

Definieren Sie eine Wiederherstellungs- und Wiederherstellungsstrategie für IBM DB2-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Ihre Datenbank wiederherstellen und wiederherstellen, damit Restore- und Recovery-Vorgänge erfolgreich durchgeführt werden können.

Es wird nur die manuelle Wiederherstellung der Datenbank unterstützt.

Schritte

1. Ermitteln Sie die Wiederherstellungsstrategien, die für manuell hinzugefügte IBM DB2-Ressourcen unterstützt werden
2. Bestimmen Sie die Wiederherstellungsstrategien, die für automatisch erkannte IBM DB2-Datenbanken unterstützt werden

Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte IBM DB2-Ressourcen unterstützt werden

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte IBM DB2-Ressourcen.

Manuell hinzugefügte IBM DB2-Ressourcen können nicht wiederhergestellt werden.

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her

Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshots, die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

Art der Wiederherstellungsstrategie, die für automatisch ermittelte IBM DB2 unterstützt wird

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können.

Vollständige Ressourcenwiederherstellung ist die Wiederherstellungsstrategie, die für automatisch erkannte IBM DB2-Datenbanken unterstützt wird. Dadurch werden alle Volumes, qtrees und LUNs einer Ressource

wiederhergestellt.

Arten von Wiederherstellungsvorgängen für automatisch ermittelte IBM DB2

Das SnapCenter Plug-in für IBM DB2 unterstützt Single File SnapRestore und Wiederherstellungstypen für Verbindungen und Kopien für automatisch erkannte IBM DB2-Datenbanken.

Ein Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn der ausgewählte Backup von einem sekundären Standort SnapMirror oder SnapVault stammt und die Option **Complete Resource** ausgewählt ist

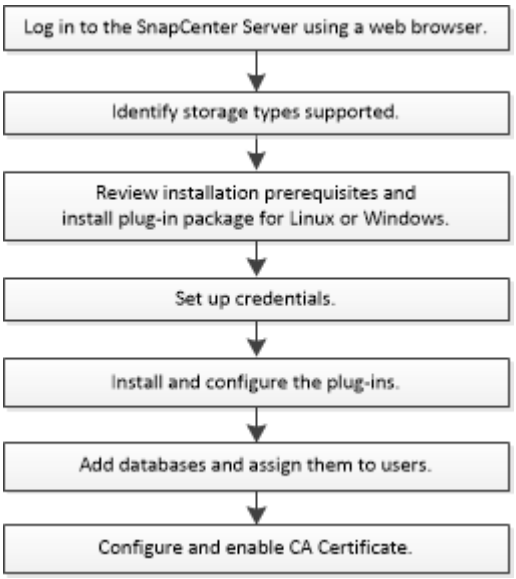
Ein Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem sekundären Standort SnapMirror oder SnapVault ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Bereiten Sie die Installation des SnapCenter-Plug-ins für IBM DB2 vor

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 das Installieren des Plug-ins-Pakets für Windows, Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-in-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Das SnapCenter Plug-in für IBM DB2 wird auf Windows-, Linux-

und AIX-Umgebungen unterstützt.

- Sie müssen Java 11 auf Ihrem Host installiert haben.

  IBM Java wird nicht unterstützt.

- Für Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „`LocalSystem`“ ausgeführt werden. Dies ist das Standardverhalten, wenn Plug-in für IBM DB2 als Domänenadministrator installiert ist.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört. Das SnapCenter-Plug-in für Microsoft Windows wird standardmäßig mit dem IBM DB2-Plug-in auf Windows-Hosts bereitgestellt.
- SnapCenter Server sollte Zugriff auf den 8145 oder benutzerdefinierten Port des Plug-ins für IBM DB2-Host haben.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Während der Installation von Plug-in 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-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-Tool"

- Für IBM DB2-Datenbanken, die auf einem Linux-Host ausgeführt werden, wird das SnapCenter-Plug-in für IBM DB2 automatisch installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-in-Installation haben.

Zusätzliche 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 eine separate Zeile ein, und bei den Befehlen wird die Groß-/Kleinschreibung nicht beachtet. Stellen Sie sicher, dass Sie den vollständig qualifizierten Pfadnamen angeben und den Pfadnamen in Anführungszeichen („) einschließen, wenn er Leerzeichen enthält.

Beispiel:

Befehl: Montieren

Befehl: Umount

Befehl: „C:\Program Files\NetApp\SnapCreator commands\sdcli.exe“

Befehl: myscript.bat

Wenn die Datei *allowed_commands.config* nicht vorhanden ist, werden die Befehle oder die Ausführung des Skripts blockiert, und der Workflow schlägt mit dem folgenden Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Wenn der Befehl oder das Skript nicht in *allowed_commands.config* vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit folgendem Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Sie sollten keinen Platzhaltereintrag (*) verwenden, um alle Befehle zuzulassen.

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter kann ein Benutzer, der kein Root-Benutzer ist, das SnapCenter-Plug-in-Paket für Linux installieren und den Plug-in-Prozess 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Stellen Sie für den Benutzer, der nicht root ist, sicher, dass der Name des Benutzers, der nicht root ist, und die Gruppe des Benutzers identisch sein sollten.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Konfigurieren Sie sudo-Berechtigungen für Benutzer, die nicht root sind, für 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_Host_Plugin.bsx
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

AIX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Host-Anforderungen 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 Speicherplatz- und Größenanforderungen des Host-Systems vertraut sein.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit der Datensicherungsvorgänge. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Anmeldedaten für das SnapCenter-Plug-in für IBM DB2 einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu

authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken oder Windows-Dateisystemen erstellen.

Über diese Aufgabe

- Linux-Hosts

  Sie müssen Anmeldedaten für die Installation von Plug-ins auf Linux-Hosts einrichten.

  Sie müssen die Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

  Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen 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 Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username* Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten. Nur für Linux-Benutzer verfügbar.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Installieren Sie das SnapCenter-Plug-in für IBM DB2

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen Hosts über die Seite SnapCenter Add Host hinzufügen hinzufügen und dann die Plug-ins-Pakete installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert. Sie können einen Host hinzufügen und Plug-in-Pakete für einen einzelnen Host oder für ein 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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zum Verwalten von Hosts.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Group Managed Service-Konto unter Windows Server 2016 oder höher für IBM DB2"

Über diese Aufgabe

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

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ aus: • Windows • Linux Das Plug-in für IBM DB2 ist auf dem IBM DB2-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System ausgeführt werden.
Host-Name	Geben Sie den Hostnamen der Kommunikation ein. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben.

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

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Wenn Sie die REST-API zum Installieren von Plug-in 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…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Installationspfad	Das Plug-in für IBM DB2 ist auf dem IBM DB2-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System ausgeführt werden. • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. Optional können Sie den Pfad anpassen. • Für das SnapCenter Plug-ins-Paket für Linux lautet der Standardpfad: /Opt/NetApp/snapcenter. Optional können Sie den Pfad anpassen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version, Speicherort (für Windows-Plug-ins) und Java 11 (für Windows- und Linux-Plug-ins) werden anhand der Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\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-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

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

9. Überwachen Sie den Installationsfortschritt.
   - Für das Windows Plug-in befinden sich die Installations- und Upgrade-Protokolle unter: *C:\Windows\SnapCenter Plug-in\Install*<JOBID>\
   - Für Linux-Plug-ins befinden sich die Installationsprotokolle unter: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log. Die Upgrade-Protokolle befinden sich unter: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log

Nachdem Sie fertig sind

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 gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

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

   Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

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 IBM DB2-Datenbank mithilfe der Benutzeroberfläche (UI) von SnapCenter installieren. Wenn Ihre Umgebung die Remote-

Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie das Plug-in für IBM DB2-Datenbank entweder im Konsolenmodus oder im unbeaufsichtigten Modus über die Befehlszeilenschnittstelle (CLI) installieren.

Bevor Sie beginnen

- Sie sollten das Plug-in für IBM DB2 Database 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 Anforderungen an die abhängige Software, die Datenbank und das Betriebssystem erfüllen.

  Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu unterstützten Konfigurationen.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Das SnapCenter-Plug-in für IBM DB2-Datenbank ist Teil des SnapCenter-Plug-ins-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins Paket für Linux installieren, sollten Sie bereits SnapCenter auf einem Windows-Host installiert haben.

Über diese Aufgabe

Wenn Parameter nicht erwähnt werden, 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 das Plug-in für IBM DB2 installiert werden soll.

   Sie können von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 HTTPS-Kommunikationsport SMCore 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 das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
   - 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 /<installation directory>/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.

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

Überwachen Sie den Status der Installation von Plug-in für IBM DB2

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

Über diese Aufgabe

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

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

Schritte

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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 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.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

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

> 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

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

   Das Standardkennwort für den 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 Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
   Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
   einfachen Namen:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
   agent.properties.
   ```

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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 SnapCenter-Plug-Ins

Über diese Aufgabe

- 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 mit dem Schlüssel CRL_PATH ändern und aktualisieren.

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

Konfigurieren Sie das CA-Zertifikat für den SnapCenter-IBM DB2-Plug-ins-Dienst auf Windows-Hosts

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 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 ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

   > Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

   C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

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

   > 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: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*

2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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 enthält:
   C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

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

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

Über diese Aufgabe

- Die neueste CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten 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* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Bereiten Sie sich auf die Datensicherung 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.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

  Sie müssen den Java-Pfad in der Umgebungspfadvariable des Host-Rechners festlegen.

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von IBM DB2 verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. 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 von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, Replizierung, Skripte und andere Eigenschaften von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

Stellen Sie sich eine Ressourcengruppe vor, die definiert, was Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Richtlinie, die definiert, wie Sie sie schützen

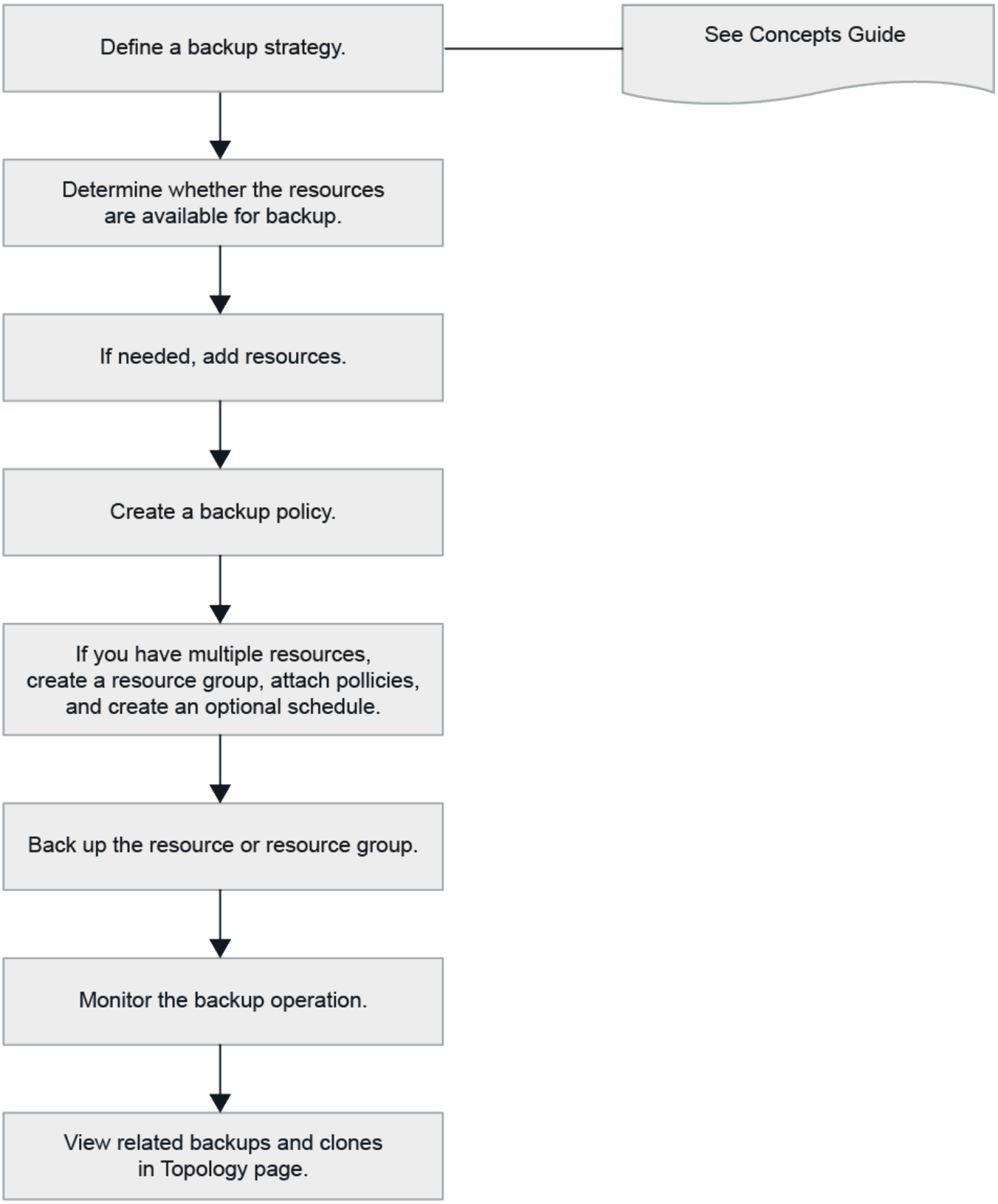
möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts umfasst. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein vollständiges Backup durchführen.

Backup von IBM DB2-Ressourcen

Backup von IBM DB2-Ressourcen

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Datenbanken, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets. "SnapCenter Software Cmdlet Referenzhandbuch".

Automatische Erkennung von Datenbanken

Bei den Ressourcen handelt es sich um IBM DB2-Datenbanken auf dem Linux-Host, die von SnapCenter gemanagt werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren IBM DB2-Datenbanken erkannt haben.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts und das Einrichten der Verbindungen des Speichersystems ausgeführt haben.
- Das SnapCenter Plug-in für IBM DB2 unterstützt keine automatische Erkennung der Ressourcen in virtuellen RDM/VMDK-Umgebungen. Sie müssen Storage-Informationen für virtuelle Umgebungen bereitstellen und gleichzeitig Datenbanken manuell hinzufügen.

Über diese Aufgabe

- 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 ermittelten 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 Ansicht 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 zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, wird in der Spalte Status insgesamt nicht geschützt angezeigt.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn kein Backup-Vorgang durchgeführt wird, wird in der Spalte Gesamtstatus der Eintrag Backup Not Run angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

Die automatische Erkennung wird auf dem Windows-Host 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.

Über diese Aufgabe

Die manuelle Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie 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 bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Datenbanknamen an.
Host-Name	Geben Sie den Hostnamen ein.
Typ	Datenbank oder Instanz auswählen.
Instanz	Geben Sie den Namen der Instanz an, die das übergeordnete Element der Datenbank ist.
Anmeldedaten	Wählen Sie die Anmeldeinformationen aus, oder fügen Sie Informationen zu den Anmeldeinformationen hinzu. Dies ist optional.

4. Wählen Sie auf der Seite „Storage Footprint bereitstellen“ einen Speichertyp aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Save**.

   Optional: Sie können auf das * -Symbol klicken , um weitere Volumes, LUNs und qtrees von anderen Storage-Systemen hinzuzufügen.

5. Optional: Geben Sie auf der Seite Ressourceneinstellungen für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für IBM DB2-Plug-in ein
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Datenbanken werden zusammen mit Informationen wie dem Hostnamen, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie den Benutzern die Ressourcen zuweisen. Auf diese Weise 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 dem Hinzufügen der Datenbanken können Sie die IBM DB2-Datenbankdetails ändern.

Backup-Richtlinien für IBM DB2 erstellen

Bevor Sie IBM DB2-Ressourcen mit SnapCenter sichern, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen finden Sie in den Informationen zur Definition einer Datensicherungsstrategie für IBM DB2-Datenbanken.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das Hinzufügen von Ressourcen ausführen.
- Der SnapCenter Administrator muss Ihnen die SVMs sowohl für die Quell- als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots zu einem Spiegel oder Vault replizieren.

  Außerdem können Sie in der Richtlinie Replizierungs-, Skript- und Applikationseinstellungen festlegen. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Über diese Aufgabe

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.
  - Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritte

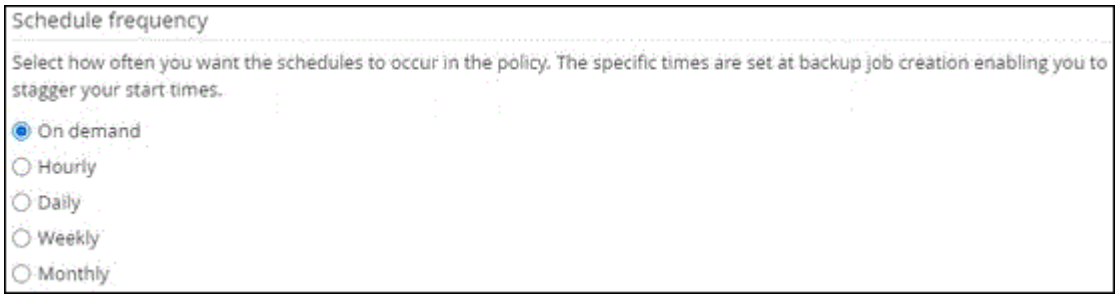
1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Richtlinientyp folgende Schritte aus:
   a. Wählen Sie den Speichertyp aus.
   b. Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-

Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.

6. Geben Sie auf der Snapshot-Seite den Zeitplantyp an, indem Sie **On Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien und Backup-Häufigkeit verwenden, aber auch die Möglichkeit haben, den einzelnen Richtlinien unterschiedliche Backup-Zeitpläne zuzuweisen.



Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

7. Geben Sie im Abschnitt Snapshot-Einstellungen die Anzahl der Snapshots an, die Sie behalten möchten.

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Kopien zu behalten** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.

Wenn Sie Snapshot Backups auf Basis von Kopien aktivieren SnapVault möchten, müssen Sie die Aufbewahrungsanzahl auf 2 oder höher festlegen. Wenn Sie die Aufbewahrungszahl auf 1 setzen, kann der Aufbewahrungsvorgang fehlschlagen, da der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

8. Geben Sie auf der Seite Aufbewahrung und Sicherung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Zeitplantyp an:
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten

sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Über diese Aufgabe

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie ein benutzerdefiniertes Namensformat für Snapshot-Kopie	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

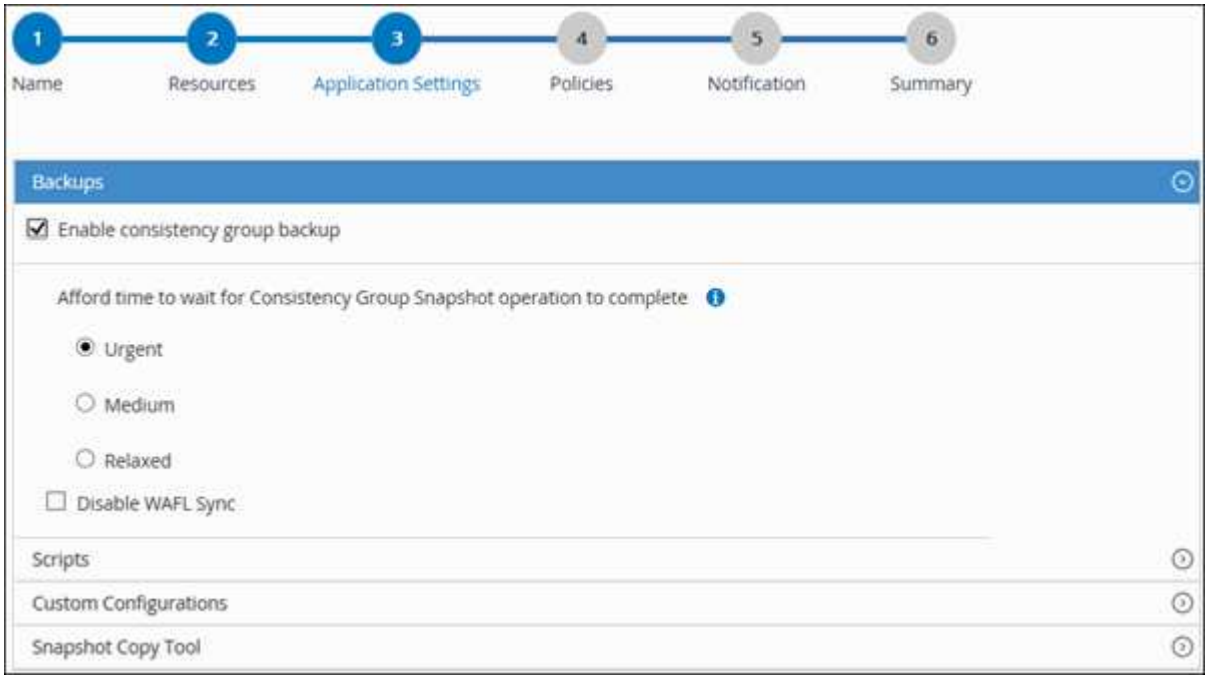
5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

   Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Warten Sie die Dauer des Snapshot-Vorgangs der Konsistenzgruppe	Wählen Sie **dringend**, **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+



a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die für alle Datenschutzvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
ARCHIVE_LOG_DIR	Change_info_Directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüssel-Wert-Paare werden für IBM DB2 Linux-Plug-in-Systeme unterstützt und nicht für IBM DB2-Datenbanken unterstützt, die als zentralisiertes Windows-Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot Copy Tool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu verwenden und das Filesystem vor dem Erstellen eines Snapshots in einen konsistenten Zustand zu versetzen. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Um den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** 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 Dropdown-Liste aus.

      Sie können eine Richtlinie auch 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 Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

      Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

      Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

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

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

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

Erstellen Sie mit PowerShell-Cmdlets für IBM DB2 eine Verbindung zum Speichersystem und Zugangsdaten

Sie müssen eine Storage Virtual Machine (SVM)-Verbindung und Zugangsdaten erstellen, bevor Sie PowerShell Cmdlets zum Sichern, Wiederherstellen oder Klonen von IBM DB2-Datenbanken verwenden.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Klicken Sie auf **SnapCenterPS**, um den PowerShell-Core zu starten.
2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel wird das Erstellen einer neuen Anmeldeinformationen namens FinanceAdmin mit Windows-Anmeldeinformationen angezeigt:

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux
-AuthenticationType PasswordBased -Credential db2hostuser
-EnableSudoPrevileges:$true
```

4. 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. Pfad auf SQLLIB festlegen.

   Für Windows verwendet das DB2-Plugin 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"}
```

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

Backup von DB2-Datenbanken

Das Sichern einer Datenbank umfasst die Einrichtung einer Verbindung mit dem SnapCenter-Server, das Hinzufügen von Ressourcen, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppen und das Sichern von Ressourcen.

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Stellen Sie für einen Backup-Vorgang mit Snapshot Kopie sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Für Pre- und Post-Befehle für Stilllegung-, Snapshot- und Stilllegung-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host über die folgenden Pfade verfügbar sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

UI von SnapCenter

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ansicht** nach Ressourcentyp.

   Wählen Sie , und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um das Filterfenster zu schließen.

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Seite Ressource **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   - Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der „Consistency Group Snapshot“-Vorgang abgeschlossen ist	Wählen Sie **dringend**, oder **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   - Wählen Sie den Pfeil von **Scripts** aus, um Pre- und Post-Befehle für Stilllegung-, Snapshot- und Unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

   - Wählen Sie den Pfeil **Custom Configurations**, und geben Sie dann die für alle Jobs, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.
   - Wählen Sie den Pfeil **Snapshot Copy Tool** aus, um das Werkzeug zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter zum Verwenden des Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen eines Snapshots einzugeben	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um einen Snapshot zu erstellen.

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

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

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

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

   b. Wählen Sie * * in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

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

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

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

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

    b. Wählen Sie **Backup**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
    - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung erkennen.

      Weitere Informationen finden Sie unter: "SnapMirror oder SnapVault-Beziehung kann nach MetroCluster Failover nicht erkannt werden"

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-SmConnection
```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Fügen Sie manuelle Ressourcen mit dem Cmdlet "Add-SmResources" 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";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\"
```

   Für Db2-Datenbank:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.
4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.
5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

   ```
   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\WINARCDB";"PluginName"="DB2"
   } -Policy db2_policy
   ```

6. Überwachen Sie den Job-Status (ausgeführt, abgeschlossen oder fehlgeschlagen) mit dem Cmdlet "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 zu Backup-Jobs wie Backup-ID, Backup-Name zum Wiederherstellen oder Klonen mit dem Cmdlet "Get-SmBackupReport".

```
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
```

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

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Über diese Aufgabe

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie , auswählen und dann das Tag auswählen. Sie können dann auswählen , um das Filterfenster 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Überwachung von IBM DB2 Backup-Vorgängen

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

Über diese Aufgabe

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

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

- Storniert

Schritte

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

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

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

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

Überwachen Sie Datenschutzvorgänge in IBM DB2-Datenbanken im Aktivitätsbereich

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

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

Schritte

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

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

Abbrechen von Backup-Vorgängen für IBM DB2

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.

- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *, um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Zeigen Sie IBM DB2-Backups und -Klone auf der Topology-Seite an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

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

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

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

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

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

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen 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 die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

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

4. Lesen Sie die **Übersichtskarte** durch, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

   Im Abschnitt **Summary Card** wird die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Clones angezeigt.

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

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

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

   Nach On-Demand-Backup, durch Klicken auf die Schaltfläche * Aktualisieren* aktualisiert die Details der Sicherung oder des Klons.

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

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

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

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

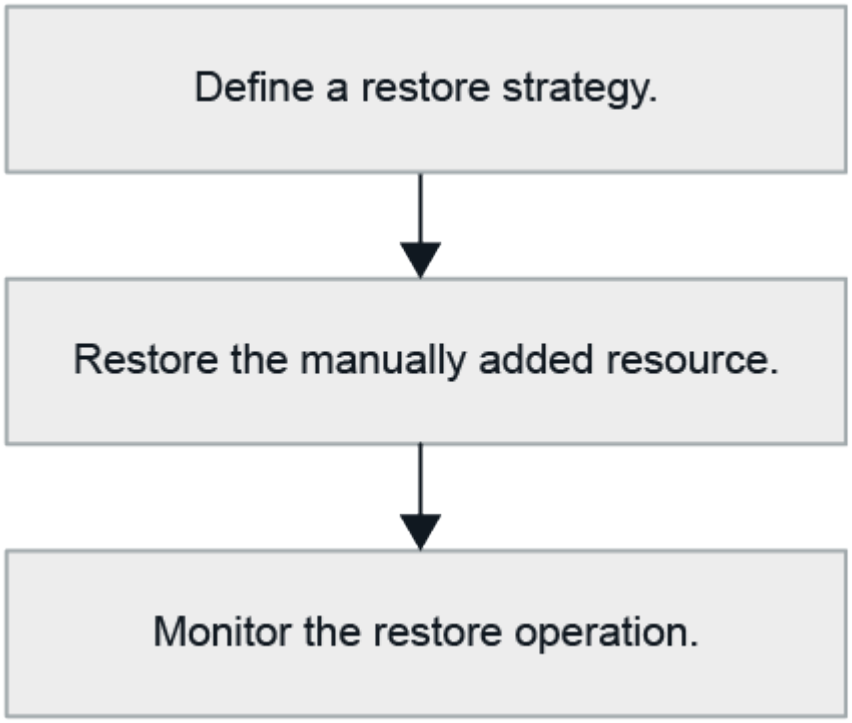
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

Stellen Sie IBM DB2 wieder her

Wiederherstellung des Workflows

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

"SnapCenter Software Cmdlet Referenzhandbuch".

Stellen Sie ein manuell hinzugefügtes Ressourcenbackup wieder her

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt

werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

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

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

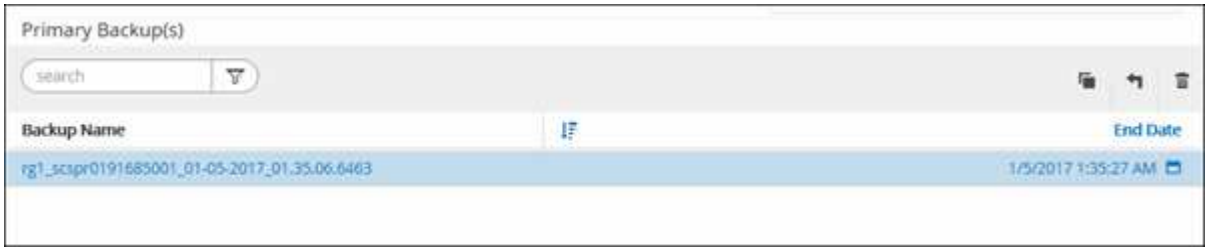
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite Wiederherstellungsbereich die Option **komplette 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 nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch 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 vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.
8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Nachdem Sie fertig sind

Die Wiederherstellung ist nur möglich, wenn der Rollforward-Status im Status „DB ausstehend“ steht. Dieser Status gilt für DB2-Datenbanken mit aktivierter Archivprotokollierung.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   PS C:\> Open-SmConnection
   ```

2. Identifizieren Sie das wiederherzustellende Backup mit den Cmdlets Get-SmBackup und Get-SmBackupReport.

   Dieses Beispiel zeigt, dass zwei Backups für die Wiederherstellung verfügbar sind:

   ```
    PS C:\> Get-SmBackup -AppObjectId
   cn24.sccore.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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

> AppObjectId ist "Host\Plugin\UID", wobei UID = <instance_name> für manuell erkannte DB2-Instanzressource und UID = <instance_name>\<databse_name> für IBM DB2-Datenbankressource ist. Sie erhalten die ResourceID aus dem Cmdlet "Get-smResources".

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode DB2
```

Dieses Beispiel zeigt, wie die Datenbank aus dem primären Speicher wiederhergestellt wird:

```
Restore-SmBackup -PluginCode DB2 -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

In diesem Beispiel wird gezeigt, wie die Datenbank aus dem sekundären Speicher wiederhergestellt wird:

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

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

Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Automatische Wiederherstellung wird nicht unterstützt.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

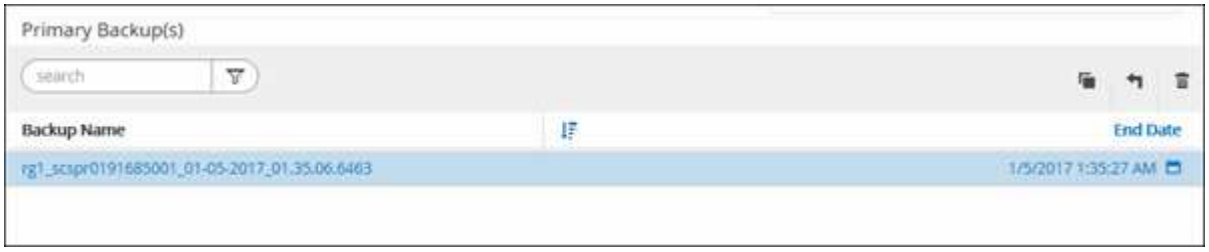
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite Wiederherstellungsumfang die Option **komplette Ressource** aus, um die konfigurierten Datenvolumes der IBM DB2-Datenbank wiederherzustellen.
7. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch ermittelte Ressourcen nicht erforderlich.

8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht erforderlich.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

Nachdem Sie fertig sind

Die Wiederherstellung ist nur möglich, wenn der Rollforward-Status im Status „DB ausstehend“ steht. Dieser Status gilt für DB2-Datenbanken mit aktivierter Archivprotokollierung.

Überwachung der IBM DB2-Wiederherstellungsvorgänge

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

Über diese Aufgabe

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

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

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

Schritte

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

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

Klonen Sie IBM DB2-Ressourcen-Backups

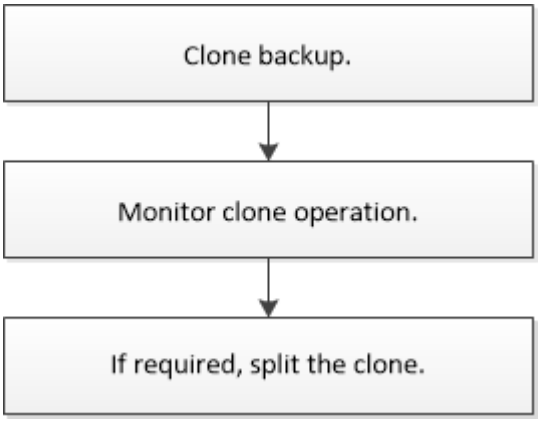
Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

- Sie können auf dem IBM DB2-Quellserver klonen.
- Sie können Ressourcen-Backups aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses
  - Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

Nachdem Sie fertig sind

Nach dem Klonen der automatisch erkannten DB2-Ressourcen wird die geklonte Ressource als manuelle Ressource markiert. Klicken Sie auf **Refresh Resources**, 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 fstab löschen.

Klonen eines IBM DB2 Backups

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen.

Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Beim Erstellen eines Klons für DB2 auf einem alternativen Host müssen Sie eine n-1-Verzeichnisstruktur

für den Mount-Pfad des Klons erstellen, die dem ursprünglichen Mount-Pfad auf dem anderen Host entspricht. Der Mount-Pfad sollte über die Ausführungsberechtigung *755* verfügen.

- Wenn Sie Befehle vor dem Klonen oder nach dem Klonen ausführen, sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host über folgende Pfade vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugeordnete 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 Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.
4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Ziel-Clone-Instanz	Geben Sie die Ziel-DB2-Clone-Instanz-ID ein, die aus den vorhandenen Backups geklont werden soll. Dies gilt nur für ANF-Speicherressource.
Name Des Ziel-Klons	Geben Sie den Namen des Klons ein. Dies gilt nur für DB2-Datenbankressource.
NFS-Export-IP-Adresse	Geben Sie IP-Adressen oder Hostnamen ein, auf denen die geklonten Volumes exportiert werden. Dies gilt nur für Ressource mit NFS-Speichertyp.
Max. Kapazitäts-Pool Durchsatz (MiB/s)	Geben Sie den maximalen Durchsatz eines Kapazitäts-Pools 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 den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
   - Befehl Pre Clone: Löschen Sie vorhandene Datenbanken mit demselben Namen
   - Befehl nach Clone: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.

b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

   Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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

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

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

Nachdem Sie fertig sind

Nach dem Klonen der automatisch erkannten DB2-Ressourcen wird die geklonte Ressource als manuelle Ressource markiert. Klicken Sie auf **Refresh Resources**, 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 fstab löschen.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Backups auf, die mit dem Cmdlet "Get-SmBackup" oder "Get-SmResourceGroup" geklont werden können.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                      BackupTime   BackupType
--------   ----------                      ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

In diesem Beispiel werden Informationen über eine bestimmte Ressourcengruppe, ihre Ressourcen und zugehörige 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}
HostResourceMaping : {}
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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup mit dem Cmdlet "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 für eine angegebene 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 Clone-Jobs mit dem Cmdlet Get-SmCloneReport an.

   In diesem Beispiel wird ein Klonbericht für die angegebene Job-ID angezeigt:

```
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}
```

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

Überwachung von IBM DB2-Klonvorgängen

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

Über diese Aufgabe

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

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

Schritte

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

Teilen Sie einen Klon auf

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

Über diese Aufgabe

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

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

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

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

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

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

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

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

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

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

   Beispiel:

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

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

Verwandte Informationen

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

Löschen oder teilen Sie IBM DB2 Datenbankklone nach dem Upgrade von SnapCenter

Nach einem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource, aus der die Klone erstellt wurden, aufteilen.

Über diese Aufgabe

Wenn Sie den Storage-Footprint der verborgenen Klone ermitteln möchten, führen Sie den folgenden Befehl aus: `Get-SmClone -ListStorageFootprint`

Schritte

1. Löschen Sie die Backups der geklonten Ressourcen mit dem Cmdlet "remove-smbackup".
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mit dem Cmdlet "remove-sresourcgruppe".
3. Entfernen Sie den Schutz der geklonten Ressource mit dem Cmdlet "remove-smprotectResource".
4. Wählen Sie auf der Seite Ressourcen die übergeordnete Ressource aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht Kopien managen die Klone entweder auf den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen 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 Host-seitige Komponente der NetApp SnapCenter Software, die ein applikationsspezifisches Datensicherungsmanagement von PostgreSQL-Clustern ermöglicht. Das Plug-in für PostgreSQL Cluster automatisiert das Backup, die Wiederherstellung und das Klonen von PostgreSQL-Clustern in einer SnapCenter-Umgebung.

SnapCenter unterstützt PostgreSQL-Konfigurationen mit einem und 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.

Nach der Installation des Plug-in für PostgreSQL-Clusters können Sie SnapCenter mit NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Mithilfe des Plug-ins in mit NetApp SnapVault Technologie lässt sich darüber hinaus eine Disk-to-Disk-Backup-Replizierung zur Einhaltung von Standards durchführen.

Das SnapCenter Plug-in für PostgreSQL unterstützt NFS und SAN unter ONTAP und Azure NetApp File Storage Layouts.

VMDK oder virtuelles Storage Layout 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 mit SnapCenter PostgreSQL-Cluster und deren Ressourcen sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Cluster hinzufügen.
- Backups erstellen.
- Restore aus Backups:
- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

Funktionen des SnapCenter Plug-in für PostgreSQL

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System 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. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore- und Klonvorgänge über alle Plug-ins hinweg, die zentralisierte Berichterstellung, die Schnellübersicht über Dashboard-Ansichten, die Einrichtung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Jobs in allen Plug-ins.

- **Automatisierte zentrale Verwaltung**

  Sie können Backup-Vorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Technologie für unterbrechungsfreie NetApp Snapshot Kopien**

  SnapCenter verwendet NetApp Snapshot-Technologie mit dem Plug-in für PostgreSQL-Cluster, um Ressourcen zu sichern.

Der Einsatz des Plug-in für PostgreSQL bietet zudem folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktgenauer Kopien von Ressourcen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Unterstützung der Snapshot-Funktion von ONTAP für Konsistenzgruppe (CG) beim Erstellen von Backups.
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Fähigkeit, Snapshots mit externen Befehlen zu erstellen.
- Unterstützung für Linux LVM auf XFS-Dateisystem.

Von SnapCenter Plug-in für PostgreSQL unterstützte Speichertypen

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines (VMs). Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter-Plug-in für PostgreSQL installieren.

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung

Maschine	Storage-Typ
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datastores • VMDKs auf VMFS • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Für das PostgreSQL-Plug-in sind mindestens ONTAP-Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun erstellen
  - lun erstellen
  - lun erstellen
  - lun löschen
  - lun Initiatorgruppe hinzufügen
  - lun-Initiatorgruppe wird erstellt
  - lun-Initiatorgruppe löschen
  - lun igroup umbenennen

- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen
- Show-Disk-Nutzung für Volume-Dateien
- Volume ist offline
- Das Volume ist online
- Volume-Änderung

    - Erstellen von Volume-qtree
    - Volume qtree löschen
    - Änderung des Volume-qtree
    - Volume-qtree anzeigen
    - Volume-Einschränkung
    - Volumen anzeigen
    - Erstellen von Volume-Snapshots
    - Volume Snapshot löschen
    - Ändern des Volume-Snapshots
    - Volume Snapshot modify-snaplock-expiry-time
    - Umbenennung von Volume-Snapshots
    - Wiederherstellung von Volume Snapshots
    - Restore-Datei für Volume Snapshots
    - Volume-Snapshot werden angezeigt
    - Volume-Aufhängung nicht verfügbar
    - cifs von vserver
    - erstellung von cifs-Freigaben von vserver
    - cifs-Freigabe von vserver: Löschen
    - vserver cifs shadowcopy anzeigen
    - cifs-Freigabe von vserver wird angezeigt
    - vserver cifs zeigen
    - vserver Exportrichtlinie
    - Erstellung von vserver Exportrichtlinien
    - vserver: Löschen der Exportrichtlinie
    - Erstellung von vserver Export-Policy-Regel
    - vserver: Export-Policy-Regel anzeigen
    - vserver Export-Policy wird angezeigt
    - vserver iscsi
    - vserver iscsi-Verbindung wird angezeigt
    - vserver zeigen
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle
    - Netzwerkschnittstelle wird angezeigt
    - vserver

Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replication für PostgreSQL vor

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie für PostgreSQL

Backup-Strategie für PostgreSQL definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre Ressourcen erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Über diese Aufgabe

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.

2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Entscheiden Sie, ob Sie eine Richtlinie auf Basis von Snapshot Kopien erstellen möchten, um applikationskonsistente Snapshots des Clusters zu sichern.
5. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
6. Legen Sie den Aufbewahrungszeitraum für die Snapshots auf dem Quell-Storage-System und dem SnapMirror Ziel fest.
7. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Automatische Ermittlung von Ressourcen auf Linux-Host

Ressourcen sind PostgreSQL-Cluster und Instanzen auf dem Linux-Host, die von SnapCenter gemanagt 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.

Art der unterstützten Backups

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot Kopien basierenden Backup-Typ für PostgreSQL Cluster.

Backup auf Basis von Snapshot Kopien

Auf Snapshot Kopien basierende Backups nutzen die NetApp Snapshot Technologie, um Online-schreibgeschützte Kopien der Volumes zu erstellen, auf denen sich die PostgreSQL-Cluster befinden.

Wie das SnapCenter Plug-in für PostgreSQL Snapshots von Konsistenzgruppen verwendet

Sie können das Plug-in verwenden, um Snapshots von Konsistenzgruppen für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes beherbergen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe ist simultane Snapshots mehrerer Volumes und stellt konsistente Kopien einer Gruppe von Volumes bereit.

Sie können auch die Wartezeit für den Speicher-Controller angeben, um Snapshots konsistent zu gruppieren. Die verfügbaren Optionen für Wartezeiten sind **dringend**, **Medium** und **entspannt**. Sie können auch die WAFL-Synchronisierung (Write Anywhere File Layout) während eines konsistenten Gruppen-Snapshots aktivieren oder deaktivieren. WAFL Sync verbessert die Performance eines Consistency Group Snapshots.

So managt SnapCenter die Organisation von Daten-Backups

SnapCenter managt die Durchführung von Daten-Backups auf der Storage-System- und File-System-Ebene.

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 Backup-Zeitplänen für PostgreSQL

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, die Service Level Agreement (SLA) und den Recovery Point Objective (RPO).

Backup-Zeitpläne haben zwei Teile:

- Backup-Häufigkeit (Häufigkeit der Durchführung von Backups)

  Die Backup-Häufigkeit, die auch als Zeitplantyp für einige Plug-ins bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau dann, wenn Backups durchgeführt werden)

  Backup-Zeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird

Anzahl der für PostgreSQL erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Backup-Namenskonventionen für Plug-in für PostgreSQL-Cluster

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Restore- und Recovery-Strategie für PostgreSQL

Definieren Sie eine Wiederherstellungs- und Wiederherstellungsstrategie für PostgreSQL-Ressourcen

Sie müssen vor dem Wiederherstellen und Wiederherstellen des Clusters eine Strategie definieren, damit Sie Wiederherstellungs- und Wiederherstellungsvorgänge erfolgreich durchführen können.

Es wird nur die manuelle Wiederherstellung des Clusters unterstützt.

Schritte

1. Ermitteln Sie die Wiederherstellungsstrategien, die für manuell hinzugefügte PostgreSQL-Ressourcen unterstützt werden
2. Ermitteln Sie die für automatisch erkannte PostgreSQL-Cluster unterstützten Wiederherstellungsstrategien
3. Geben Sie die Art der Recovery-Vorgänge an, die Sie ausführen möchten.

Arten von Wiederherstellungsstrategien, die für manuell hinzugefügte PostgreSQL-Ressourcen unterstützt werden

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können.

Manuell hinzugefügte PostgreSQL-Ressourcen können nicht wiederhergestellt werden.

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her

Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshots, die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

HINWEIS: Plug-in für PostgreSQL erstellt ein Backup_Label und tablespace_map im Ordner */<OS_temp_folder>/postgresql_sc_Recovery*<Restore_JobId>/_, um die manuelle Wiederherstellung zu unterstützen.

Art der Wiederherstellungsstrategie, die für automatisch erkannte PostgreSQL unterstützt wird

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können.

Vollständige Ressourcenwiederherstellung ist die Wiederherstellungsstrategie, die für automatisch erkannte PostgreSQL-Cluster unterstützt wird. Dadurch werden alle Volumes, qtrees und LUNs einer Ressource

wiederhergestellt.

Arten von Wiederherstellungsvorgängen für automatisch erkannte PostgreSQL

Das SnapCenter Plug-in für PostgreSQL unterstützt Single File SnapRestore und stellt Wiederherstellungsarten für automatisch erkannte PostgreSQL-Cluster her.

Ein Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn der ausgewählte Backup von einem sekundären Standort SnapMirror oder SnapVault stammt und die Option **Complete Resource** ausgewählt ist

Ein Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem sekundären Standort SnapMirror oder SnapVault 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.

- Stellen Sie den Cluster bis zum letzten Status wieder her
- Wiederherstellung des Clusters bis zu einem bestimmten Zeitpunkt

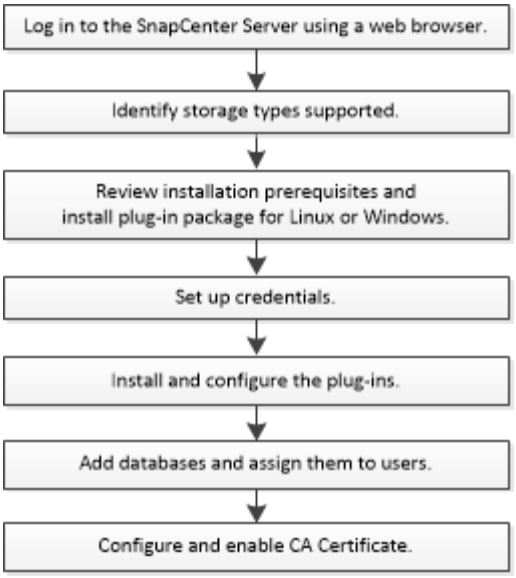
  Sie müssen Datum und Uhrzeit für die Wiederherstellung angeben.

SnapCenter bietet auch die Option Keine Wiederherstellung für PostgreSQL-Cluster.

Bereiten Sie die Installation des SnapCenter-Plug-ins für PostgreSQL vor

Installationsworkflow des SnapCenter Plug-in für PostgreSQL

Sie sollten das SnapCenter-Plug-in für PostgreSQL installieren und einrichten, wenn Sie PostgreSQL-Cluster schützen möchten.



Voraussetzungen, um Hosts hinzuzufügen und das SnapCenter-Plug-in für PostgreSQL zu installieren

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 nicht unterstützt.

- Für Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „`LocalSystem`“ ausgeführt werden. Dies ist das Standardverhalten, wenn Plug-in for PostgreSQL als Domänenadministrator installiert wird.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört. Das SnapCenter-Plug-in für Microsoft Windows wird standardmäßig mit dem PostgreSQL-Plug-in auf Windows-Hosts implementiert.
- SnapCenter Server sollte Zugriff auf den 8145 oder benutzerdefinierten Port des Plug-in für PostgreSQL-Hosts haben.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Während der Installation von Plug-in 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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-Tool"

- Bei PostgreSQL-Clustern, die auf einem Linux-Host ausgeführt werden, wird das SnapCenter-Plug-in für UNIX automatisch installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-in-Installation haben.

Zusätzliche Befehle

Um einen zusätzlichen Befehl auf dem SnapCenter Plug-in für PostgreSQL auszuführen, müssen Sie ihn in die Datei *allowed_commands.config* einfügen.

- 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 eine separate Zeile ein, und bei den Befehlen wird die Groß-/Kleinschreibung nicht beachtet. 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 Ausführung des Skripts blockiert, und der Workflow schlägt mit dem folgenden Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Wenn der Befehl oder das Skript nicht in *allowed_commands.config* vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit folgendem Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Sie sollten keinen Platzhaltereintrag (*) verwenden, um alle Befehle zuzulassen.

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter 2.0 und höheren Versionen kann ein nicht-Root-Benutzer das SnapCenter Plug-ins-Paket für Linux installieren und das Plug-in-Verfahren 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Stellen Sie für den Benutzer, der nicht root ist, sicher, dass der Name des Benutzers, der nicht root ist, und die Gruppe des Benutzers identisch sein sollten.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- _C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_plugins_checksum.txt _ wenn SnapCenter-Server auf dem Windows-Host installiert ist.
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• DOTNET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Host-Anforderungen 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 Speicherplatz- und Größenanforderungen des Host-Systems vertraut sein.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit der Datensicherungsvorgänge. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Anmeldedaten für das SnapCenter-Plug-in für PostgreSQL einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldeinformationen für die Durchführung von Datensicherungsvorgängen auf Clustern oder Windows-Filesystemen erstellen.

Über diese Aufgabe

- Linux-Hosts

Sie müssen Anmeldedaten für die Installation von Plug-ins auf Linux-Hosts einrichten.

Sie müssen die Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen 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 Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username* Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten. Nur für Linux-Benutzer verfügbar.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Installieren Sie das SnapCenter-Plug-in für PostgreSQL

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen Hosts über die Seite SnapCenter Add Host hinzufügen hinzufügen und dann die Plug-ins-Pakete 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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.

- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zum Verwalten von Hosts.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Group Managed Service-Konto unter Windows Server 2016 oder höher für PostgreSQL"

Über diese Aufgabe

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

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ aus: • Windows • Linux Das Plug-in für PostgreSQL wird auf dem PostgreSQL-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System ausgeführt werden.
Host-Name	Geben Sie den Hostnamen der Kommunikation ein. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben.

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

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Wenn Sie das Plug-in für PostgreSQL mit der REST-API installieren, müssen Sie die Version als 3.0 übergeben. Beispiel: PostgreSQL:3.0

6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Installationspfad	Das Plug-in für PostgreSQL wird auf dem PostgreSQL-Client-Host installiert, und dieser Host kann entweder auf einem Windows-System oder auf einem Linux-System ausgeführt werden. • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. Optional können Sie den Pfad anpassen. • Für das SnapCenter Plug-ins-Paket für Linux lautet der Standardpfad: /Opt/NetApp/snapcenter. Optional können Sie den Pfad anpassen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Fügen Sie alle Hosts im Cluster hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten hinzuzufügen.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden mit den Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\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-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

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

9. Überwachen Sie den Installationsfortschritt.
   - Für das Windows Plug-in befinden sich die Installations- und Upgrade-Protokolle unter: *C:\Windows\SnapCenter Plug-in\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 befinden sich 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 gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

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

   Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Installieren Sie das SnapCenter-Plug-in für PostgreSQL auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten das SnapCenter-Plug-in für PostgreSQL-Cluster mithilfe der

Benutzeroberfläche (UI) von SnapCenter installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie das Plug-in für PostgreSQL-Cluster entweder im Konsolenmodus oder im unbeaufsichtigten Modus über die 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 PostgreSQL-Cluster installieren, muss die Anforderungen an die abhängige Software, den Cluster und das Betriebssystem erfüllen.

  Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu unterstützten Konfigurationen.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Das SnapCenter-Plug-in für PostgreSQL-Cluster ist Teil des SnapCenter-Plug-ins-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins Paket für Linux installieren, sollten Sie bereits SnapCenter 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 von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 HTTPS-Kommunikationsport SMCore 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 das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
   - 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 /<installation directory>/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.

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

Überwachen Sie den Status der Installation von Plug-in für PostgreSQL

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

Über diese Aufgabe

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

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

Schritte

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

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten

CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

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

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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks
```

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
keytool -list -v -keystore keystore.jks
```

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

   Das Standardkennwort für den 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 Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
agent.properties.
```

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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 SnapCenter-Plug-Ins

Über diese Aufgabe

- 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 mit dem Schlüssel CRL_PATH ändern und aktualisieren.

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL 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 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 ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

   > Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

   C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

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

   > 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:

C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc

2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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 enthält: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

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

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

Über diese Aufgabe

- Die neueste CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten 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* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

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

Bevor Sie beginnen

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

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

Schritte

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

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.

- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Bereiten Sie sich auf die Datensicherung 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.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

  Sie müssen den Java-Pfad in der Umgebungspfadvariable des Host-Rechners festlegen.

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von PostgreSQL verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei Ressourcen handelt es sich in der Regel 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 von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, Replizierung, Skripte und andere Eigenschaften von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

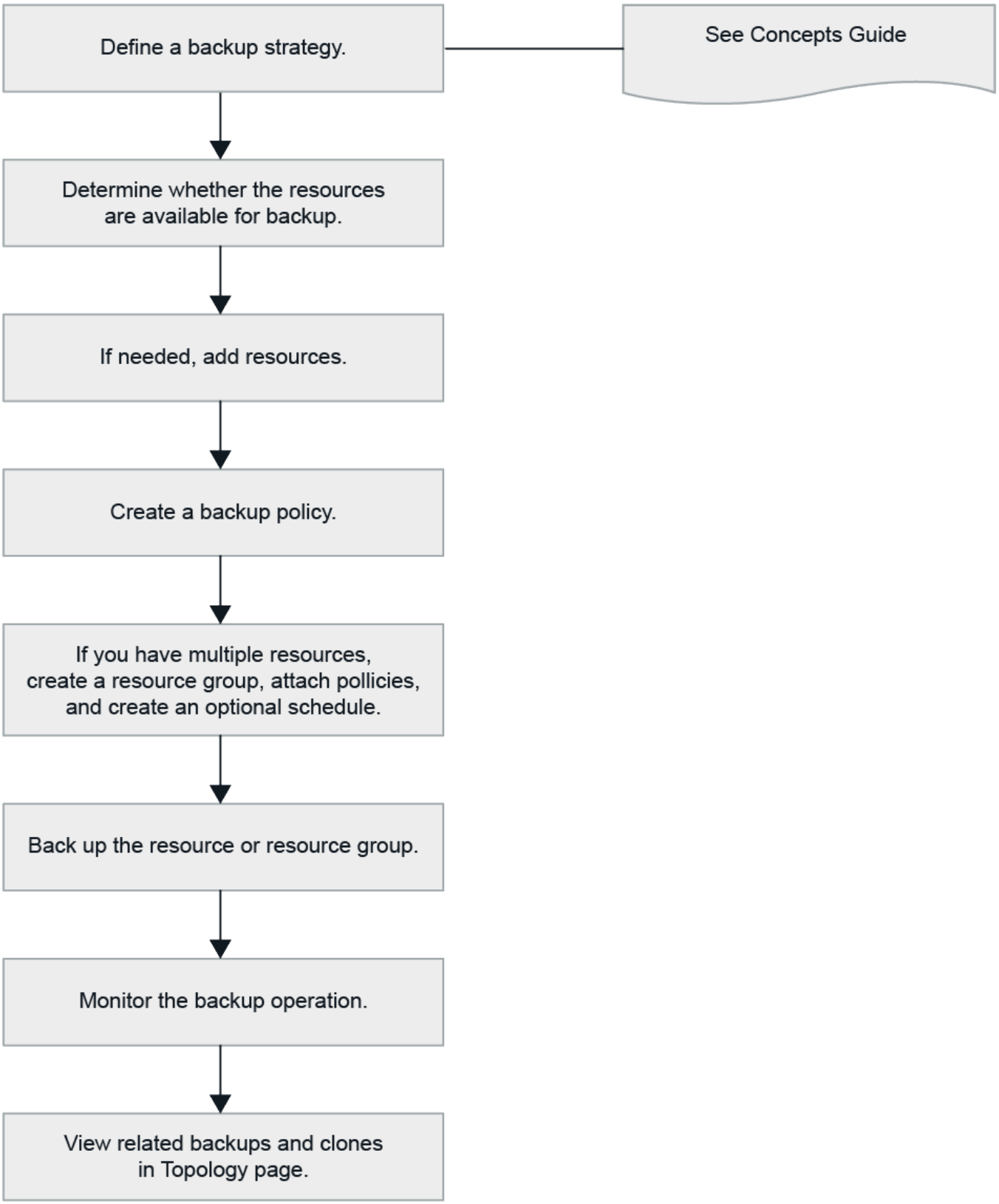
Stellen Sie sich eine Ressourcengruppe vor, die definiert, was Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Richtlinie, die definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Cluster sichern, können Sie eine Ressourcengruppe erstellen, die alle Cluster im Host umfasst. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein vollständiges Backup durchführen.

Sichern Sie PostgreSQL-Ressourcen

Sichern Sie PostgreSQL-Ressourcen

Sie können entweder ein Backup einer Ressource (eines Clusters) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Cluster, das Management von Backup-Richtlinien, die Erstellung von Ressourcengruppen und das Anhängen von Richtlinien, die Erstellung von Backups und die Überwachung von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets. "SnapCenter Software Cmdlet Referenzhandbuch".

Automatische Erkennung der Cluster

Ressourcen sind PostgreSQL-Cluster auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren PostgreSQL-Cluster erkannt haben.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts und das Einrichten der Verbindungen des Speichersystems ausgeführt haben.
- Das SnapCenter Plug-in für PostgreSQL unterstützt keine automatische Erkennung der Ressourcen in virtuellen RDM/VMDK-Umgebungen.

Über diese Aufgabe

- 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 ermittelten 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 Ansicht 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 zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich das Cluster auf einem NetApp-Speicher befindet und nicht geschützt ist, wird in der Spalte Gesamtstatus nicht geschützt angezeigt.
   - Wenn sich das Cluster auf einem NetApp-Speichersystem befindet und geschützt ist und kein Backup durchgeführt wird, wird in der Spalte Gesamtstatus die Meldung Sicherung nicht ausgeführt angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

Sie müssen die Ressourcen aktualisieren, wenn die Cluster außerhalb von SnapCenter umbenannt werden.

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

Die automatische Erkennung wird auf dem Windows-Host nicht unterstützt. Sie müssen PostgreSQL-Cluster-Ressourcen 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.

Über diese Aufgabe

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 bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Cluster-Namen an.
Host-Name	Geben Sie den Hostnamen ein.
Typ	Wählen Sie Cluster aus.
Instanz	Geben Sie den Namen der Instanz an, die das übergeordnete Objekt des Clusters ist.
Anmeldedaten	Wählen Sie die Anmeldeinformationen aus, oder fügen Sie Informationen zu den Anmeldeinformationen hinzu. Dies ist optional.

4. Wählen Sie auf der Seite „Storage Footprint bereitstellen“ einen Speichertyp aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Save**.

   Optional: Sie können auf das * -Symbol klicken , um weitere Volumes, LUNs und qtrees von anderen Storage-Systemen hinzuzufügen.

5. Optional: Geben Sie auf der Seite Resource Settings für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für PostgreSQL-Plug-in ein
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Cluster werden zusammen mit Informationen wie dem Hostnamen, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie den Benutzern die Ressourcen zuweisen. Auf diese Weise 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 fertig sind

- Nachdem Sie die Cluster hinzugefügt haben, können Sie die Details zum PostgreSQL-Cluster ändern.
- Die migrierten Ressourcen (Tablespace und Cluster) von SnapCenter 5.0 werden in SnapCenter 6.0 als PostgreSQL-Cluster-Typ gekennzeichnet.
- Wenn Sie die manuell hinzugefügten Ressourcen ändern, die von SnapCenter 5.0 oder früher migriert werden, gehen Sie auf der Seite **Ressourceneinstellungen** für benutzerdefinierte Schlüsselwertpaare folgendermaßen vor:
  - Geben Sie den Begriff "PORT" im Feld **Name** an.
  - Geben Sie die Portnummer im Feld **Wert** an.

Erstellen Sie Backup-Richtlinien für PostgreSQL

Bevor Sie PostgreSQL-Ressourcen mit SnapCenter sichern, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen finden Sie unter Definieren einer Datensicherungsstrategie für PostgreSQL-Cluster.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das Hinzufügen von Ressourcen ausführen.
- Der SnapCenter Administrator muss Ihnen die SVMs sowohl für die Quell- als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots zu einem Spiegel oder Vault replizieren.

  Außerdem können Sie in der Richtlinie Replizierungs-, Skript- und Applikationseinstellungen festlegen. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Über diese Aufgabe

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.
  - Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

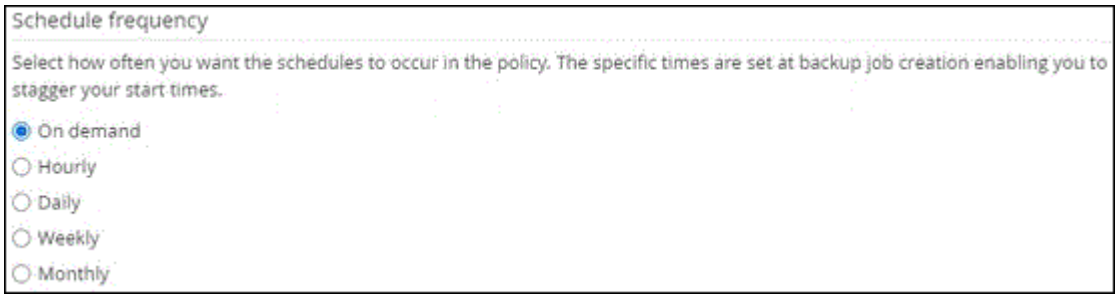
Schritte

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 Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Richtlinientyp folgende Schritte aus:
   a. Wählen Sie den Speichertyp aus.
   b. Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

      Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.
6. Geben Sie auf der Snapshot-Seite den Zeitplantyp an, indem Sie **On Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

   Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien und Backup-Häufigkeit verwenden, aber auch die Möglichkeit haben, den einzelnen Richtlinien unterschiedliche Backup-Zeitpläne zuzuweisen.



   Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.
7. Geben Sie im Abschnitt Snapshot-Einstellungen die Anzahl der Snapshots an, die Sie behalten möchten.
8. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Kopien zu behalten** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.

Wenn Sie Snapshot Backups auf Basis von Kopien aktivieren SnapVault möchten, müssen Sie die Aufbewahrungsanzahl auf 2 oder höher festlegen. Wenn Sie die Aufbewahrungszahl auf 1 setzen, kann der Aufbewahrungsvorgang fehlschlagen, da der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Über diese Aufgabe

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.

Für dieses Feld…	Tun Sie das…
Verwenden Sie ein benutzerdefiniertes Namensformat für Snapshot-Kopie	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Warten Sie die Dauer des Snapshot-Vorgangs der Konsistenzgruppe	Wählen Sie **dringend**, **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+

a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die für alle Datenschutzvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
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 Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüssel-Wert-Paare werden für PostgreSQL Linux Plug-in-Systeme unterstützt und nicht für PostgreSQL Cluster unterstützt, die als zentralisiertes Windows Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot Copy Tool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu verwenden und das Filesystem vor dem Erstellen eines Snapshots in einen konsistenten Zustand zu versetzen. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Um den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** 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 Dropdown-Liste aus.

Sie können eine Richtlinie auch 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 Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

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

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

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

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

Erstellen Sie mit PowerShell Cmdlets für PostgreSQL eine Verbindung zum Speichersystem und Zugangsdaten

Sie müssen eine Storage Virtual Machine (SVM)-Verbindung und Zugangsdaten erstellen, bevor Sie mit PowerShell Cmdlets PostgreSQL-Cluster sichern, wiederherstellen oder klonen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

Host-Plug-in-Installationen dürfen während des Hinzufügens einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Cluster-Status möglicherweise in der SnapCenter-GUI als „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Starten Sie eine PowerShell Core-Verbindungssitzung mit dem Cmdlet "Open-SmConnection".

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel wird das Erstellen einer neuen Anmeldeinformationen namens FinanceAdmin mit Windows-Anmeldeinformationen angezeigt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Fügen Sie den PostgreSQL-Kommunikationshost dem 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. Pfad auf SQLLIB festlegen.

   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”}
```

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

Sichern Sie PostgreSQL

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

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Stellen Sie für Backup-Vorgänge auf Basis von Snapshot Kopien sicher, dass alle Mandanten-Cluster gültig und aktiv sind.
- Für Pre- und Post-Befehle für Stilllegung-, Snapshot- und Stilllegung-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host über die folgenden Pfade verfügbar sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

UI von SnapCenter

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ansicht** nach Ressourcentyp.

   Wählen Sie , und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um das Filterfenster zu schließen.

3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Seite Ressource **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   - Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der „Consistency Group Snapshot“-Vorgang abgeschlossen ist	Wählen Sie **dringend**, oder **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   - Wählen Sie den Pfeil von **Scripts** aus, um Pre- und Post-Befehle für Stilllegung-, Snapshot- und Unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

   - Wählen Sie den Pfeil **Custom Configurations**, und geben Sie dann die für alle Jobs, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.
   - Wählen Sie den Pfeil **Snapshot Copy Tool** aus, um das Werkzeug zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter zum Verwenden des Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen eines Snapshots einzugeben	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um einen Snapshot zu erstellen.

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

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

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

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

   b. Wählen Sie * * in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

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

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

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

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

    b. Wählen Sie **Backup**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
    - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

      Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der 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 auf Folgendes: *Java -jar -Xmx8192M -Xms4096M*

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   PS C:\> Open-SmConnection
   ```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Fügen Sie manuelle Ressourcen mit dem Cmdlet "Add-SmResources" 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 mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.
4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.
5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

   ```
   C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Dieses Beispiel sichert eine geschützte Ressource:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

6. Überwachen Sie den Job-Status (ausgeführt, abgeschlossen oder fehlgeschlagen) mit dem Cmdlet "Get-smJobSummaryReport".

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Überwachen Sie die Details zu Backup-Jobs wie Backup-ID, Backup-Name zum Wiederherstellen oder Klonen mit dem Cmdlet "Get-SmBackupReport".

```
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 :
```

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

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Über diese Aufgabe

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie , auswählen und dann das Tag auswählen. Sie können dann auswählen , um das Filterfenster 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

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

   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Überwachen von PostgreSQL-Backup-Vorgängen

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

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.

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

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

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

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

Überwachen Sie Datensicherungsvorgänge auf PostgreSQL-Clustern im Aktivitätsbereich

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

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

Schritte

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

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

Backup-Vorgänge für PostgreSQL abbrechen

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite

Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *, um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Zeigen Sie PostgreSQL-Backups und Clones auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

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

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

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

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

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen 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 die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

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

4. Lesen Sie die **Übersichtskarte** durch, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

   Im Abschnitt **Summary Card** wird die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Clones angezeigt.

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

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

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

   Nach On-Demand-Backup, durch Klicken auf die Schaltfläche * Aktualisieren* aktualisiert die Details der Sicherung oder des Klons.

5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf die Datensicherungssymbole, um Restore-, Klon- und Löschvorgänge durchzuführen.

Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

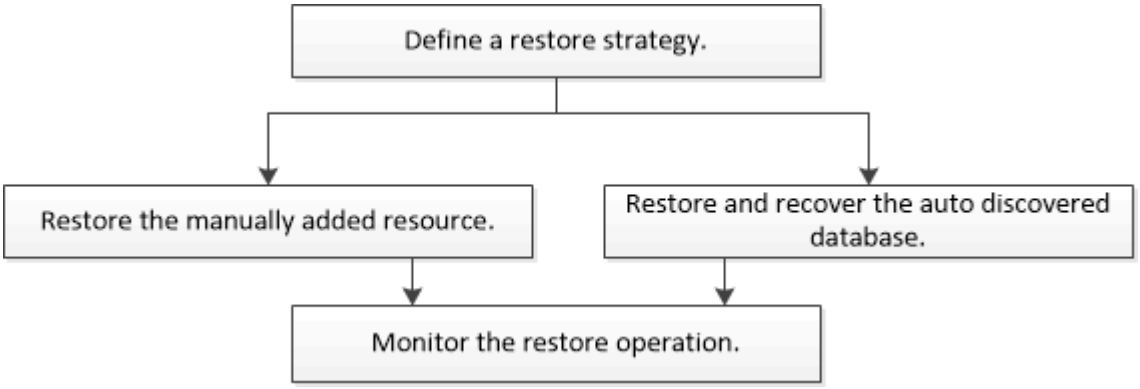
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

PostgreSQL wiederherstellen

Wiederherstellung des Workflows

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

"SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

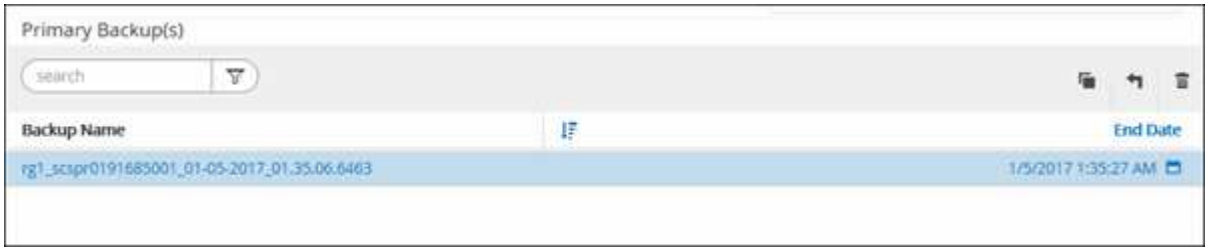
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite Wiederherstellungsbereich die Option **komplette 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 nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch 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 vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellung und Wiederherstellung einer automatisch erkannten Cluster-Sicherung

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem

unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:

- 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Dateibasierte Backup-Kopien können nicht aus SnapCenter wiederhergestellt werden.
- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Automatische Wiederherstellung wird nicht unterstützt.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

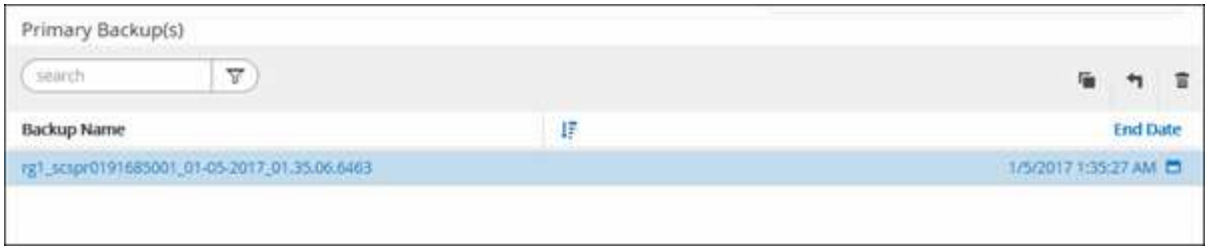
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite Wiederherstellungsumfang die Option **komplette Ressource** aus, um die konfigurierten Datenvolumes des PostgreSQL-Clusters wiederherzustellen.
7. Wählen Sie auf der Seite Recovery Scope eine der folgenden Optionen aus:

Sie suchen…	Tun Sie das…
Möchten so nah wie möglich bis zur aktuellen Zeit wiederherstellen	Wählen Sie **Wiederherstellen in aktuellster Zustand**. Bei einzelnen Container-Ressourcen legen Sie einen oder mehrere Backup-Standorte für Protokolle und Kataloge fest.
Wiederherstellung auf den angegebenen Zeitpunkt	Wählen Sie **Wiederherstellen zu Zeitpunkt**. a. Geben Sie Datum und Uhrzeit ein. Geben Sie Datum und Uhrzeit ein. Der PostgreSQL Linux-Host befindet sich beispielsweise in Sunnyvale, Kalifornien, und der Benutzer in Raleigh, NC, stellt die Protokolle in SnapCenter wieder her. Wenn der Benutzer eine Wiederherstellung auf 5 a.m durchführen will. Sunnyvale, CA, dann muss der Benutzer die Browser-Zeitzone auf die PostgreSQL Linux-Host-Zeitzone einstellen, die GMT-07:00 ist und das Datum und die Uhrzeit als 5:00 Uhr angeben
Möchten Sie nicht wiederherstellen	Wählen Sie **Keine Wiederherstellung**.

Manuell hinzugefügte PostgreSQL-Ressourcen können nicht wiederhergestellt werden.

Das SnapCenter-Plugin für PostgreSQL erstellt ein Backup_Label und eine Tablespace_Map im Ordner */<OS_temp_folder>/postgresql_sc_Recovery*<Restore_JobId>/_, um eine manuelle Wiederherstellung zu ermöglichen.

1. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

2. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

3. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

4. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                 : Restore
'scc54.sccore.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           :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen Sie die PostgreSQL-Wiederherstellungsvorgänge

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

-  In Bearbeitung

- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Klonen von PostgreSQL-Ressourcen-Backups

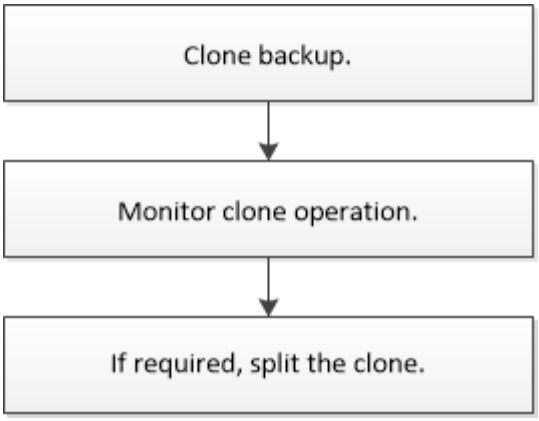
Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

- Sie können auf dem PostgreSQL-Quellserver klonen.
- Sie können Ressourcen-Backups aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses
  - Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

Klonen eines PostgreSQL-Backups

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen.

Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Wenn Sie Befehle vor dem Klonen oder nach dem Klonen ausführen, sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host über folgende Pfade vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugeordnete 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 Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.
4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Zielport	Geben Sie den PostgreSQL-Zielport ein, der aus den vorhandenen Backups geklont werden soll.
NFS-Export-IP-Adresse	Geben Sie IP-Adressen oder Hostnamen ein, auf denen die geklonten Volumes exportiert werden. Dies gilt nur für Ressource mit NFS-Speichertyp.
Max. Kapazitäts-Pool Durchsatz (MiB/s)	Geben Sie den maximalen Durchsatz eines Kapazitäts-Pools ein. Dies gilt nur für ANF-Speicherressource.

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 den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
      - Pre Clone, Befehl: Löschen Sie vorhandene Cluster mit demselben Namen
      - Post Clone-Befehl: Überprüfen Sie ein Cluster oder starten Sie ein Cluster.

b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:

Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-SmConnection
```

2. Rufen Sie die Backups für den Klonvorgang mit dem Cmdlet Get-SmBackup ab.

   Dieses Beispiel zeigt, dass zwei Backups 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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

   Dieses Beispiel zeigt, dass das zu klonende Backup über eine NFSExportIPs-Adresse 10.32.212.14 verfügt:

   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 sind, wird der Standardwert auf den Klon-Zielhost exportiert.

4. Überprüfen Sie, ob die Backups erfolgreich geklont wurden, indem Sie das Cmdlet "Get-SmCloneReport" verwenden, um die Details zu den Klonjobs anzuzeigen.

   Sie können Details wie Klon-ID, Startdatum und -Zeit, Enddatum und -Zeit 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 Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Teilen Sie einen Klon auf

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon ist unabhängig von der übergeordneten Ressource.

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** die entsprechende Option aus der Liste Ansicht aus:

Option	Beschreibung
Für Datenbankapplikationen	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Für File-Systeme	Wählen Sie in der Liste Ansicht **Pfad** aus.

3. Wählen Sie die entsprechende Ressource aus der Liste aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Clone-Splitvorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet "Stop-SmJob" ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragzeit benötigen, um zu prüfen, ob der Klon geteilt ist oder nicht, können Sie den Wert von *CloneSplitStatusCheckPollTime* Parameter in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Clone Split-Vorgangs angezeigt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klontrennung schlägt fehl, wenn gerade Backup-, Wiederherstellungs- oder andere Klonsplitonen durchgeführt werden. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Verwandte Informationen

"Der SnapCenter Klon oder die Überprüfung schlägt fehl, wenn das Aggregat nicht vorhanden ist"

Löschen oder teilen Sie PostgreSQL Cluster Clones nach dem Upgrade von SnapCenter

Nach einem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource, aus der die Klone erstellt wurden, aufteilen.

Über diese Aufgabe

Wenn Sie den Storage-Footprint der verborgenen Klone ermitteln möchten, führen Sie den folgenden Befehl aus: `Get-SmClone -ListStorageFootprint`

Schritte

1. Löschen Sie die Backups der geklonten Ressourcen mit dem Cmdlet "remove-smbackup".
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mit dem Cmdlet "remove-sresourcgruppe".
3. Entfernen Sie den Schutz der geklonten Ressource mit dem Cmdlet "remove-smprotectResource".
4. Wählen Sie auf der Seite Ressourcen die übergeordnete Ressource aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht Kopien managen die Klone entweder auf den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen 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 Datenbank ist eine Host-seitige Komponente der NetApp SnapCenter Software, die ein applikationsspezifisches Datensicherungs-Management von MySQL Datenbanken ermöglicht. Das Plug-in für MySQL Database automatisiert das Backup, die Wiederherstellung und das Klonen von MySQL-Datenbanken in einer SnapCenter Umgebung.

SnapCenter unterstützt MySQL-Setups mit einer Instanz. Sie können das Plug-in für MySQL Database sowohl in Linux- als auch in Windows-Umgebungen verwenden. In Windows-Umgebungen wird MySQL als manuelle Ressource unterstützt.

Nach der Installation des Plug-in für MySQL-Datenbanken können Sie mithilfe von SnapCenter mit NetApp SnapMirror Technologie gespiegelte Kopien von Backup-Sets auf einem anderen Volume erstellen. Mithilfe des Plug-ins in mit NetApp SnapVault Technologie lässt sich darüber hinaus eine Disk-to-Disk-Backup-Replizierung zur Einhaltung von Standards durchführen.

Das SnapCenter Plug-in für MySQL unterstützt NFS und SAN unter ONTAP und Azure NetApp File Storage Layouts.

VMDK oder virtuelles Storage Layout 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-Datenbank in Ihrer Umgebung installieren, können Sie mit SnapCenter MySQL-Instanzen sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Fügen Sie Instanzen hinzu.
- Backups erstellen.
- Restore aus Backups:
- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

SnapCenter Plug-in für MySQL Funktionen

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Um mit dem Plug-in für MySQL-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. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore- und Klonvorgänge über alle Plug-ins hinweg, die zentralisierte Berichterstellung, die Schnellübersicht über Dashboard-Ansichten, die Einrichtung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Jobs in allen Plug-ins.

- **Automatisierte zentrale Verwaltung**

  Sie können Backup-Vorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Technologie für unterbrechungsfreie NetApp Snapshot Kopien**

  SnapCenter nutzt NetApp Snapshot Technologie mit dem Plug-in für MySQL Datenbank, um Ressourcen zu sichern.

Die Verwendung des Plug-ins für MySQL bietet zudem folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktgenauer Kopien von Ressourcen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Unterstützung der Snapshot-Funktion von ONTAP für Konsistenzgruppe (CG) beim Erstellen von Backups.
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Fähigkeit, Snapshots mit externen Befehlen zu erstellen.
- Unterstützung für Linux LVM auf XFS-Dateisystem.

Vom SnapCenter-Plug-in für MySQL unterstützte Storage-Typen

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines (VMs). Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie das SnapCenter-Plug-in für MySQL installieren.

Maschine	Storage-Typ
Physischer Server	• FC-verbundene LUNs • ISCSI-verbundene LUNs • Volumes mit NFS-Anbindung
VMware ESXi	• RDM-LUNs, die über ein FC- oder iSCSI-ESXi HBASCAning der Host Bus Adapter (HBAs) verbunden sind, können viel Zeit in Anspruch nehmen, da SnapCenter alle im Host vorhandenen Host-Bus-Adapter scannt. Sie können die Datei **LinuxConfig.pm** unter */opt/NetApp/snapcenter/spl/Plugins/scu/scucore/modules/SCU/Config* bearbeiten, um den Wert des **SCSI_HOSTS_OPTIMIZED_RECAN** Parameters auf 1 zu setzen, um nur die in HBA_DRIVER_NAMES aufgeführten HBAs erneut zu scannen. • ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind • VMDKs auf NFS-Datastores • VMDKs auf VMFS erstellt • NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Für das MySQL Plug-in sind minimale ONTAP-Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun
  - lun erstellen
  - lun erstellen
  - lun erstellen
  - lun löschen

- lun Initiatorgruppe hinzufügen
- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- lun Persistent-Reservierung löschen
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen

    - Show-Disk-Nutzung für Volume-Dateien
    - Volume ist offline
    - Das Volume ist online
    - Volume-Änderung
    - Erstellen von Volume-qtree
    - Volume qtree löschen
    - Änderung des Volume-qtree
    - Volume-qtree anzeigen
    - Volume-Einschränkung
    - Volumen anzeigen
    - Erstellen von Volume-Snapshots
    - Volume Snapshot löschen
    - Ändern des Volume-Snapshots
    - Volume Snapshot modify-snaplock-expiry-time
    - Umbenennung von Volume-Snapshots
    - Wiederherstellung von Volume Snapshots
    - Restore-Datei für Volume Snapshots
    - Volume-Snapshot werden angezeigt
    - Volume-Aufhängung nicht verfügbar
    - cifs von vserver
    - erstellung von cifs-Freigaben von vserver
    - cifs-Freigabe von vserver: Löschen
    - vserver cifs shadowcopy anzeigen
    - cifs-Freigabe von vserver wird angezeigt
    - vserver cifs zeigen
    - vserver Exportrichtlinie
    - Erstellung von vserver Exportrichtlinien
    - vserver: Löschen der Exportrichtlinie
    - Erstellung von vserver Export-Policy-Regel
    - vserver: Export-Policy-Regel anzeigen
    - vserver Export-Policy wird angezeigt
    - vserver iscsi
    - vserver iscsi-Verbindung wird angezeigt
    - vserver zeigen
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle
    - Netzwerkschnittstelle wird angezeigt

- vserver

Bereiten Sie die Storage-Systeme für SnapMirror und SnapVault Replizierung für MySQL vor

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie für MySQL

Backup-Strategie für MySQL definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre Ressourcen erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Über diese Aufgabe

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.
2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Entscheiden Sie, ob Sie eine Richtlinie für auf Snapshot Kopien basierende erstellen möchten, um applikationskonsistente Snapshots der Datenbank zu sichern.
5. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
6. Legen Sie den Aufbewahrungszeitraum für die Snapshots auf dem Quell-Storage-System und dem SnapMirror Ziel fest.
7. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Automatische Ermittlung von Ressourcen auf Linux-Host

Bei den Ressourcen handelt es sich um MySQL-Instanzen auf dem Linux-Host, die von SnapCenter gemanagt werden. Nach der Installation des SnapCenter Plug-ins für MySQL werden die MySQL-Instanzen auf diesem Linux-Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Art der unterstützten Backups

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt den auf Snapshot Kopien basierenden Backup-Typ für MySQL-Datenbanken.

Backup auf Basis von Snapshot Kopien

Auf Snapshot Kopien basierende Backups nutzen die NetApp Snapshot Technologie, um Online-schreibgeschützte Kopien der Volumes zu erstellen, auf denen sich die MySQL-Datenbanken befinden.

Wie das SnapCenter Plug-in für MySQL Snapshots von Konsistenzgruppen verwendet

Sie können das Plug-in verwenden, um Snapshots von Konsistenzgruppen für Ressourcengruppen zu erstellen. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes beherbergen kann, sodass Sie sie als eine Einheit verwalten können. Eine Konsistenzgruppe ist simultane Snapshots mehrerer Volumes und stellt konsistente Kopien einer Gruppe von Volumes bereit.

Sie können auch die Wartezeit für den Speicher-Controller angeben, um Snapshots konsistent zu gruppieren. Die verfügbaren Optionen für Wartezeiten sind **dringend**, **Medium** und **entspannt**. Sie können auch die WAFL-Synchronisierung (Write Anywhere File Layout) während eines konsistenten Gruppen-Snapshots aktivieren oder deaktivieren. WAFL Sync verbessert die Performance eines Consistency Group Snapshots.

So managt SnapCenter die allgemeine Ordnung und Sauberkeit von Protokoll-Backups

SnapCenter managt die Durchführung von Daten-Backups auf der Storage-System- und File-System-Ebene.

Überlegungen zur Festlegung von Backup-Zeitplänen für MySQL

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, die Service Level Agreement (SLA) und den Recovery Point Objective (RPO).

Backup-Zeitpläne haben zwei Teile:

- Backup-Häufigkeit (Häufigkeit der Durchführung von Backups)

  Die Backup-Häufigkeit, die auch als Zeitplantyp für einige Plug-ins bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren.

- Backup-Zeitpläne (genau dann, wenn Backups durchgeführt werden)

  Backup-Zeitpläne sind Teil einer Ressourcen- oder Ressourcengruppenkonfiguration. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird

Anzahl der Backup-Jobs, die für MySQL benötigt werden

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Backup-Namenskonventionen für Plug-in für MySQL-Datenbanken

Sie können entweder die standardmäßige Snapshot-Namenskonvention verwenden oder eine benutzerdefinierte Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt Snapshot Namen einen Zeitstempel hinzu, der Ihnen dabei hilft, zu ermitteln, wann die Kopien erstellt wurden.

Für den Snapshot wird die folgende Standard-Namenskonvention verwendet:

```
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 Bedeutungen:

- *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 Schutz von Ressourcen oder Ressourcengruppen angeben, indem Sie **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** auswählen. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird dem Snapshot-Namen das Suffix mit dem Zeitstempel hinzugefügt.

Restore- und Recovery-Strategie für MySQL

Definieren Sie eine Restore- und Recovery-Strategie für MySQL-Ressourcen

Sie müssen eine Strategie definieren, bevor Sie Ihre Datenbank wiederherstellen und wiederherstellen, damit Restore- und Recovery-Vorgänge erfolgreich durchgeführt werden können.

Es wird nur die manuelle Wiederherstellung der Datenbank unterstützt.

Schritte

1. Ermitteln Sie die Wiederherstellungsstrategien, die für manuell hinzugefügte MySQL-Ressourcen unterstützt werden
2. Ermitteln Sie die Wiederherstellungsstrategien, die für automatisch erkannte MySQL-Datenbanken unterstützt werden
3. Geben Sie die Art der Recovery-Vorgänge an, die Sie ausführen möchten.

Typen von Wiederherstellungsstrategien, die für manuell hinzugefügte MySQL-Ressourcen unterstützt werden

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können. Es gibt zwei Arten von Wiederherstellungsstrategien für manuell hinzugefügte MySQL-Ressourcen.

Manuell hinzugefügte MySQL-Ressourcen können nicht wiederhergestellt werden.

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her

Wenn die Ressource Volumes oder qtrees enthält, werden die Snapshots, die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellt wurden, gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

Typ der Wiederherstellungsstrategie, die für automatisch ermitteltes MySQL unterstützt wird

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge mit SnapCenter erfolgreich durchführen können.

Eine vollständige Wiederherstellung der Ressourcen ist die Wiederherstellungsstrategie, die für automatisch erkannte MySQL-Datenbanken unterstützt wird. Dadurch werden alle Volumes, qtrees und LUNs einer Ressource wiederhergestellt.

Arten von Wiederherstellungsvorgängen für automatisch ermitteltes MySQL

Das SnapCenter Plug-in für MySQL unterstützt einzelne Datei-SnapRestore und Wiederherstellungsarten für Verbindungen und Kopien für automatisch erkannte MySQL-Datenbanken.

Ein Single File SnapRestore wird in NFS-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn der ausgewählte Backup von einem sekundären Standort SnapMirror oder SnapVault stammt und die Option **Complete Resource** ausgewählt ist

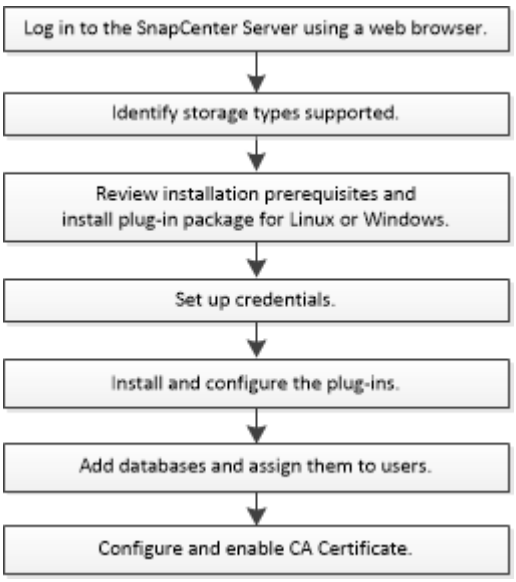
Ein Single File SnapRestore wird in SAN-Umgebungen für die folgenden Szenarien ausgeführt:

- Wenn nur die Option **Complete Resource** ausgewählt ist
- Wenn das Backup von einem sekundären Standort SnapMirror oder SnapVault ausgewählt wird und die Option **Complete Resource** ausgewählt ist

Bereiten Sie die Installation des SnapCenter-Plug-ins für MySQL vor

Installationsworkflow des SnapCenter Plug-ins für MySQL

Sie sollten das SnapCenter-Plugin für MySQL installieren und einrichten, wenn Sie MySQL-Datenbanken schützen möchten.



Voraussetzungen, um Hosts hinzuzufügen und das SnapCenter-Plug-in für MySQL zu installieren

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 nicht unterstützt.

- Für Windows sollte der Plug-in Creator Service mit dem Windows-Benutzer „`LocalSystem`“ ausgeführt werden. Dies ist das Standardverhalten, wenn Plug-in für MySQL als Domänenadministrator installiert wird.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört. 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 mysql config (my.cnf oder mysql-Server.cnf) angegeben werden.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Während der Installation von Plug-in 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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-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.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-Tool"

- Bei MySQL-Datenbanken, die auf einem Linux-Host ausgeführt werden, wird das SnapCenter-Plug-in für MySQL automatisch installiert.
- Sie sollten **bash** als Standard-Shell für die Plug-in-Installation haben.

Zusätzliche Befehle

Um einen zusätzlichen Befehl auf dem SnapCenter-Plugin für MySQL auszuführen, müssen Sie ihn in die Datei *allowed_commands.config* einfügen.

- 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 eine separate Zeile ein, und bei den Befehlen wird die Groß-/Kleinschreibung nicht beachtet. 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 Ausführung des Skripts blockiert, und der Workflow schlägt mit dem folgenden Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Wenn der Befehl oder das Skript nicht in *allowed_commands.config* vorhanden ist, wird die Ausführung des Befehls oder Skripts blockiert und der Workflow schlägt mit folgendem Fehler fehl:

„[/mnt/Mount -a] Ausführung nicht zulässig. Autorisieren Sie, indem Sie den Befehl in der Datei %s auf dem Plugin-Host hinzufügen.“

Sie sollten keinen Platzhaltereintrag (*) verwenden, um alle Befehle zuzulassen.

Konfigurieren von Sudo-Berechtigungen für Benutzer ohne Root-Zugriff auf Linux-Hosts

Mit SnapCenter 2.0 und höheren Versionen kann ein nicht-Root-Benutzer das SnapCenter Plug-ins-Paket für Linux installieren und das Plug-in-Verfahren 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 umask 0027 ist, stellen Sie sicher, dass der java-Ordner und alle darin enthaltenen Dateien die Berechtigung 555 haben sollten. Andernfalls kann die Installation des Plug-ins fehlschlagen.
- Stellen Sie für den Benutzer, der nicht root ist, sicher, dass der Name des Benutzers, der nicht root ist, und die Gruppe des Benutzers identisch sein sollten.
- Bearbeiten Sie die Datei */etc/ssh/sshd_config*, um die Algorithmen für den Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- _C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_plugins_checksum.txt _ wenn SnapCenter-Server auf dem Windows-Host installiert ist.
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• DOTNET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Host-Anforderungen 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 Speicherplatz- und Größenanforderungen des Host-Systems vertraut sein.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit der Datensicherungsvorgänge. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist. Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Anmeldedaten für das SnapCenter-Plug-in für MySQL einrichten

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in Datenbanken oder Windows-Dateisystemen erstellen.

Über diese Aufgabe

- Linux-Hosts

  Sie müssen Anmeldedaten für die Installation von Plug-ins auf Linux-Hosts einrichten.

  Sie müssen die Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

  Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen 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 Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Credential die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username* Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus, den Sie verwenden möchten.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten. Nur für Linux-Benutzer verfügbar.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Installieren Sie das SnapCenter-Plug-in für MySQL

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen Hosts über die Seite SnapCenter Add Host hinzufügen hinzufügen und dann die Plug-ins-Pakete 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:
  - Führen Sie ein Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher durch
  - Führen Sie ein Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher durch
- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Die Administrationsdokumentation enthält Informationen zum Verwalten von Hosts.

Über diese Aufgabe

- 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. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ aus: • Windows • Linux Das Plug-in für MySQL muss auf dem MySQL-Datenbankserver installiert werden.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den Hostnamen der Kommunikation ein. Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben.
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Wenn Sie das Plug-in für MySQL mit der REST-API installieren, müssen Sie die Version als 3.0 übergeben. Beispiel: MySQL:3.0

6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.

Für dieses Feld…	Tun Sie das…
Installationspfad	Das Plug-in für MySQL ist auf dem MySQL-Client-Host installiert, und dieser Host kann sich entweder auf einem Windows-System oder auf einem Linux-System befinden. • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. Optional können Sie den Pfad anpassen. • Für das SnapCenter Plug-ins-Paket für Linux lautet der Standardpfad: /Opt/NetApp/snapcenter. Optional können Sie den Pfad anpassen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Fügen Sie alle Hosts im Cluster hinzu	Keine Angabe.
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Keine Angabe.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen überspringen nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden mit den Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter C:\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-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

   Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.
    - Für das Windows Plug-in befinden sich die Installations- und Upgrade-Protokolle unter: *C:\Windows\SnapCenter Plug-in\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 befinden sich unter: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Nachdem Sie fertig sind

Wenn Sie auf SnapCenter 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 gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

Sie müssen sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie das Plug-in-Paket installieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

    Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

    Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Installieren Sie das SnapCenter-Plug-in für MySQL auf Linux-Hosts über die Befehlszeilenschnittstelle

Sie sollten das SnapCenter-Plug-in für die MySQL-Datenbank über die SnapCenter-Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie das Plug-in für MySQL-Datenbank entweder im Konsolenmodus oder im unbeaufsichtigten Modus über die Befehlszeilenschnittstelle (CLI) installieren.

Bevor Sie beginnen

- Sie sollten das Plug-in für MySQL Database auf jedem Linux-Host installieren, auf dem die MySQL-Instanz geschützt werden muss.

- Der Linux-Host, auf dem Sie das SnapCenter-Plug-in für die MySQL-Datenbank installieren, muss die Anforderungen an die abhängige Software, die Datenbank und das Betriebssystem erfüllen.

  Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu unterstützten Konfigurationen.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Das SnapCenter-Plug-in für die MySQL-Datenbank ist Teil des SnapCenter-Plug-ins-Pakets für Linux. Bevor Sie das SnapCenter Plug-ins Paket für Linux installieren, sollten Sie bereits SnapCenter 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\Paket-Repository auf den Host, auf dem Sie das Plug-in für MySQL installieren möchten.

   Sie können von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 HTTPS-Kommunikationsport SMCore 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 das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
   - 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 /<installation directory>/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.

   Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen Sie den Status der Installation von Plug-in für MySQL

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden, gehen Sie wie folgt vor:
   a. Klicken Sie Auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

```
 keytool -storepasswd -keystore keystore.jks
. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im
Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher
verwendet wird:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen 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. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.

7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das Standardkennwort für den 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 Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
   Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
   einfachen Namen:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
   agent.properties.
   ```

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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 SnapCenter-Plug-Ins

Über diese Aufgabe

- 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 mit dem Schlüssel CRL_PATH ändern und aktualisieren.

   Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL 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 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 ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

   Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

   C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

4. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

   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: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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 enthält: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen 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. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

Über diese Aufgabe

- Die neueste CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten 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* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Bereiten Sie sich auf die Datensicherung 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.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.

- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten erstellen.
- Installieren Sie Java 11 auf Ihrem Linux- oder Windows-Host.

  Sie müssen den Java-Pfad in der Umgebungspfadvariable des Host-Rechners festlegen.

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von MySQL verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Bei Ressourcen handelt es sich in der Regel 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 von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, Replizierung, Skripte und andere Eigenschaften von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

Stellen Sie sich eine Ressourcengruppe vor, die definiert, was Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Richtlinie, die definiert, wie Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken des Hosts umfasst. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein vollständiges Backup durchführen.

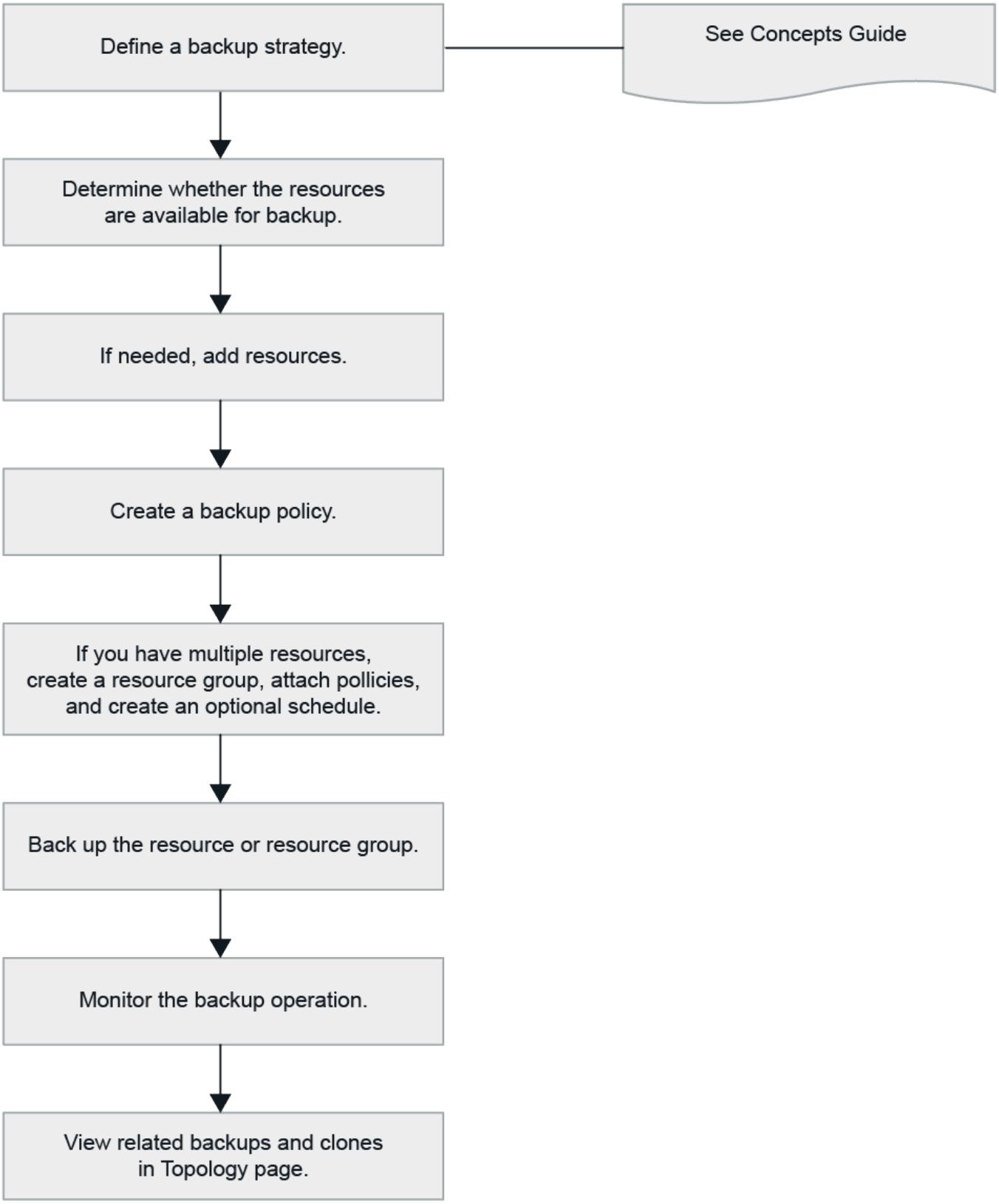
Backup von MySQL Ressourcen

Backup von MySQL Ressourcen

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Datenbanken, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und

das Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet

Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets. "SnapCenter Software Cmdlet Referenzhandbuch".

Automatische Erkennung von Datenbanken

Bei den Ressourcen handelt es sich um MySQL-Datenbanken auf dem Linux-Host, die von SnapCenter gemanagt werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren MySQL-Datenbanken erkannt haben.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts und das Einrichten der Verbindungen des Speichersystems ausgeführt haben.
- Das SnapCenter Plug-in für MySQL unterstützt nicht die automatische Erkennung von Ressourcen in virtuellen RDM/VMDK-Umgebungen. Sie müssen Storage-Informationen für virtuelle Umgebungen bereitstellen und gleichzeitig Datenbanken manuell hinzufügen.

Über diese Aufgabe

- 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 ermittelten 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 Ansicht 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 zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, wird in der Spalte Status insgesamt nicht geschützt angezeigt.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn kein Backup-Vorgang durchgeführt wird, wird in der Spalte Gesamtstatus der Eintrag Backup Not Run angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

Sie müssen die Ressourcen aktualisieren, wenn die Instanzen außerhalb von SnapCenter umbenannt werden.

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

Die automatische Erkennung wird auf dem Windows-Host 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-Plugin 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 bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Datenbanknamen an.
Host-Name	Geben Sie den Hostnamen ein.
Typ	Wählen Sie eine Instanz aus.
Instanz	Keine Angabe.
Anmeldedaten	Wählen Sie die Anmeldeinformationen aus, oder fügen Sie Informationen zu den Anmeldeinformationen hinzu. Dies ist optional.

4. Wählen Sie auf der Seite „Storage Footprint bereitstellen“ einen Speichertyp aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Save**.

   Optional: Sie können auf das * -Symbol klicken  , um weitere Volumes, LUNs und qtrees von anderen Storage-Systemen hinzuzufügen.

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 stellen**.

   Die Datenbanken werden zusammen mit Informationen wie dem Hostnamen, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie den Benutzern die Ressourcen zuweisen. Auf diese Weise 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 dem Hinzufügen der Datenbanken können Sie die MySQL-Datenbankdetails ändern.

Backup-Richtlinien für MySQL erstellen

Bevor Sie SnapCenter zum Sichern von MySQL-Ressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Bevor Sie beginnen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen finden Sie im Artikel zur Definition einer Datensicherungsstrategie für MySQL-Datenbanken.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das Hinzufügen von Ressourcen ausführen.
- Der SnapCenter Administrator muss Ihnen die SVMs sowohl für die Quell- als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots zu einem Spiegel oder Vault replizieren.

  Außerdem können Sie in der Richtlinie Replizierungs-, Skript- und Applikationseinstellungen festlegen. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Über diese Aufgabe

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.
  - Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

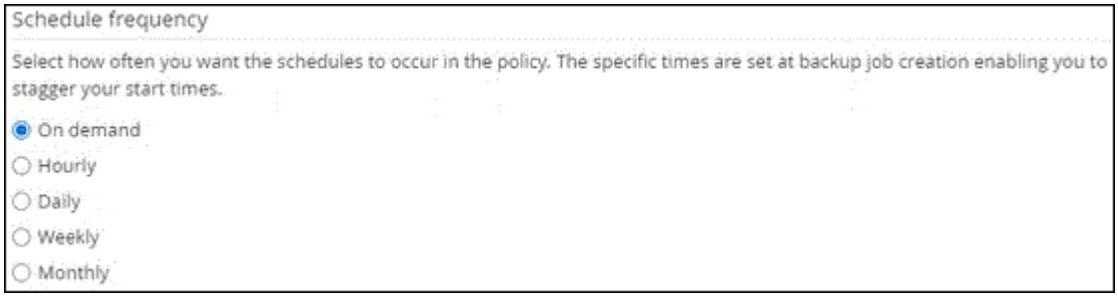
Schritte

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 Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Richtlinientyp folgende Schritte aus:
   a. Wählen Sie den Speichertyp aus.
   b. Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

      Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.

6. Geben Sie auf der Snapshot-Seite den Zeitplantyp an, indem Sie **On Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien und Backup-Häufigkeit verwenden, aber auch die Möglichkeit haben, den einzelnen Richtlinien unterschiedliche Backup-Zeitpläne zuzuweisen.



Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

7. Geben Sie im Abschnitt Snapshot-Einstellungen die Anzahl der Snapshots an, die Sie behalten möchten.
8. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Kopien zu behalten** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.

Wenn Sie Snapshot Backups auf Basis von Kopien aktivieren SnapVault möchten, müssen Sie die Aufbewahrungsanzahl auf 2 oder höher festlegen. Wenn Sie die Aufbewahrungszahl auf 1 setzen, kann der Aufbewahrungsvorgang fehlschlagen, da der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des

Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Über diese Aufgabe

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein.  Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie ein benutzerdefiniertes Namensformat für Snapshot-Kopie	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

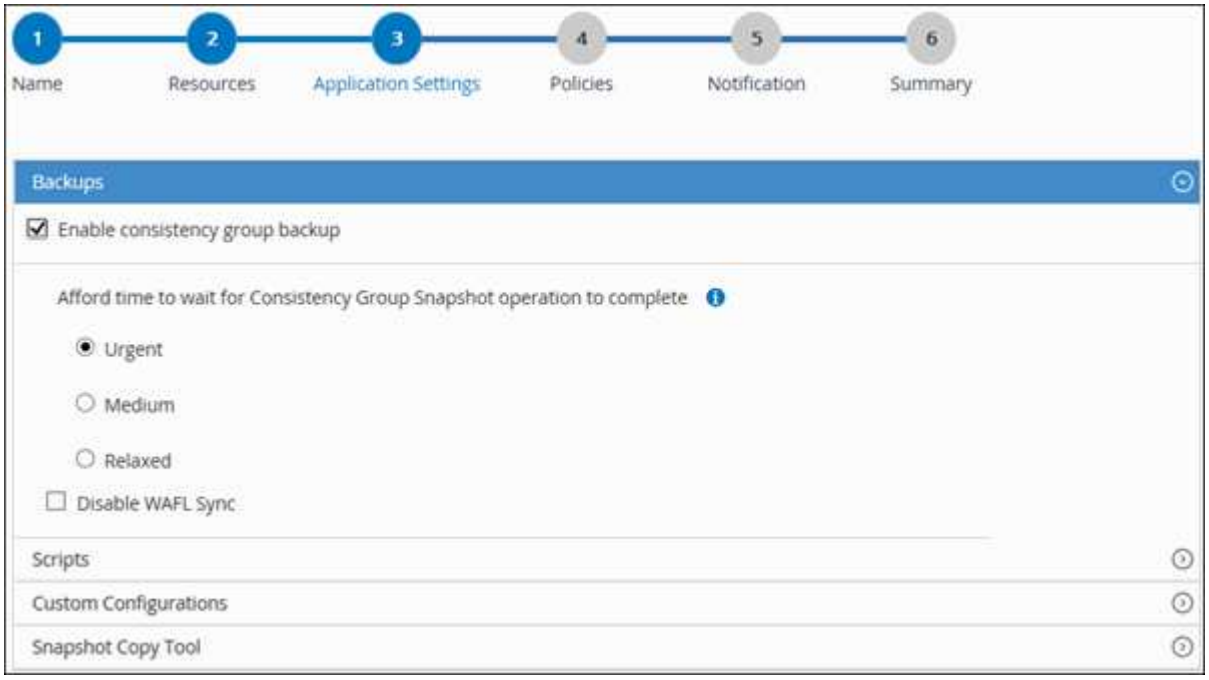
5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Warten Sie die Dauer des Snapshot-Vorgangs der Konsistenzgruppe	Wählen Sie **dringend**, **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+



a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die für alle Datenschutzvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
ARCHIVE_LOG_DIR	Change_info_Directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüssel-Wert-Paare werden für MySQL Linux-Plug-in-Systeme unterstützt und nicht für MySQL-Datenbanken unterstützt, die als zentralisiertes Windows-Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot Copy Tool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu verwenden und das Filesystem vor dem Erstellen eines Snapshots in einen konsistenten Zustand zu versetzen. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Um den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** 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 Dropdown-Liste aus.

      Sie können eine Richtlinie auch 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 Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

      Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

      Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

   Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen Sie eine Storage-Systemverbindung und Zugangsdaten mit PowerShell Cmdlets für MySQL

Sie müssen eine Storage Virtual Machine (SVM)-Verbindung und Zugangsdaten erstellen, bevor Sie PowerShell Cmdlets zum Backup, zur Wiederherstellung oder zum Klonen von MySQL-Datenbanken verwenden.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Starten Sie eine PowerShell Core-Verbindungssitzung mit dem Cmdlet "Open-SmConnection".

```
PS C:\> Open-SmConnection
```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel wird das Erstellen einer neuen Anmeldeinformationen namens FinanceAdmin mit Windows-Anmeldeinformationen angezeigt:

```
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. Pfad auf SQLLIB festlegen.

   Für Windows verwendet das MySQL-Plugin 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”}
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Backup von MySQL

Wenn eine Ressource noch nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Stellen Sie für einen Backup-Vorgang mit Snapshot Kopie sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Für Pre- und Post-Befehle für Stilllegung-, Snapshot- und Stilllegung-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host über die folgenden Pfade verfügbar sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

UI von SnapCenter

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ansicht** nach Ressourcentyp.

   Wählen Sie , und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um das Filterfenster zu schließen.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Seite Ressource **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.
5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   - Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der „Consistency Group Snapshot“-Vorgang abgeschlossen ist	Wählen Sie **dringend**, oder **Mittel** oder **entspannt**, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   - Wählen Sie den Pfeil von **Scripts** aus, um Pre- und Post-Befehle für Stilllegung-, Snapshot- und Unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.
   - Wählen Sie den Pfeil **Custom Configurations**, und geben Sie dann die für alle Jobs, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.
   - Wählen Sie den Pfeil **Snapshot Copy Tool** aus, um das Werkzeug zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter zum Verwenden des Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen eines Snapshots einzugeben	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um einen Snapshot zu erstellen.

6. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf * * klicken .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Wählen Sie * * in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann **OK** aus.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

9. Wählen Sie **Jetzt sichern**.
10. Führen Sie auf der Seite Backup die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

       Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

    b. Wählen Sie **Backup**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
    - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

      Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der 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 auf Folgendes: *Java -jar -Xmx8192M -Xms4096M*

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-SmConnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Fügen Sie manuelle Ressourcen mit dem Cmdlet "Add-SmResources" 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 mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.
4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.
5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

   ```
   C:\PS> New-SmBackup -Resources
   @{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
   luginName"="MySQL"} -Policy "MySQL_snapshotbased"
   ```

   Dieses Beispiel sichert eine geschützte Ressource:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
   -Policy mysql_policy2
   ```

6. Überwachen Sie den Job-Status (ausgeführt, abgeschlossen oder fehlgeschlagen) mit dem Cmdlet "Get-smJobSummaryReport".

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Überwachen Sie die Details zu Backup-Jobs wie Backup-ID, Backup-Name zum Wiederherstellen oder Klonen mit dem Cmdlet "Get-SmBackupReport".

```
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 :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Über diese Aufgabe

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie , auswählen und dann das Tag auswählen. Sie können dann auswählen , um das Filterfenster 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Monitoring von MySQL Backup-Vorgängen

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.

3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Obwohl der Status des Sicherungsauftrags angezeigt wird , wird beim Klicken auf Jobdetails möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen Sie Datensicherungsvorgänge bei MySQL Instanzen im Teilfenster „Aktivität“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Job-Details** aufgeführt.

Backup-Vorgänge für MySQL abbrechen

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite

Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *, um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Zeigen Sie MySQL-Backups und -Klone auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

-  Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.

Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen 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 die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Lesen Sie die **Übersichtskarte** durch, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

   Im Abschnitt **Summary Card** wird die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Clones angezeigt.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

   Wenn ein SnapLock-fähiges Backup durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die primäre und sekundäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen wird. Ein wöchentlicher Zeitplan aktualisiert auch die primäre und sekundäre SnapLock-Ablaufzeit, die von ONTAP abgerufen wird.

   Wenn die Applikationsressource über mehrere Volumes verteilt ist, ist die SnapLock-Ablaufzeit für das Backup die längste SnapLock-Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock-Ablaufzeit wird von ONTAP abgerufen.

   Nach On-Demand-Backup, durch Klicken auf die Schaltfläche * Aktualisieren* aktualisiert die Details der Sicherung oder des Klons.

5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf die Datensicherungssymbole, um Restore-, Klon- und Löschvorgänge durchzuführen.

Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

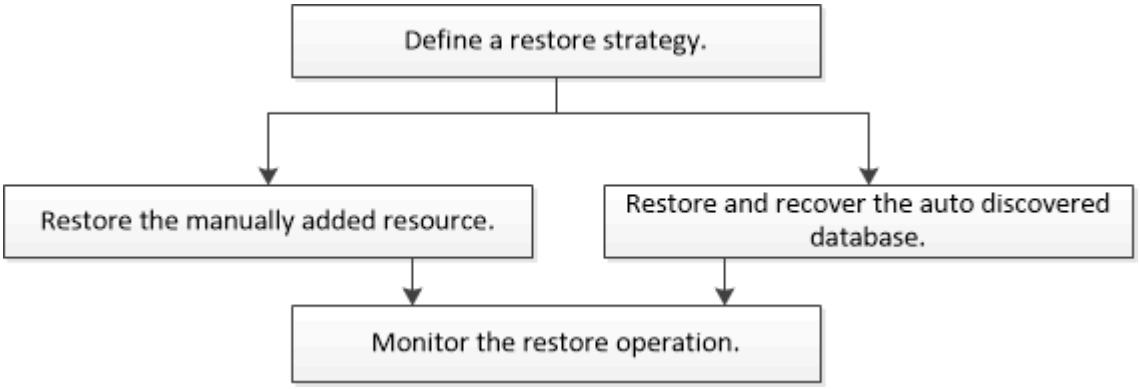
7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .

Stellen Sie MySQL wieder her

Wiederherstellung des Workflows

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring von Vorgängen.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

"SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines manuell hinzugefügten Ressourcen-Backups

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Bei ONTAP 9.12.1 und älteren Versionen übernehmen die aus den SnapLock Vault Snapshots im Rahmen der Wiederherstellung erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

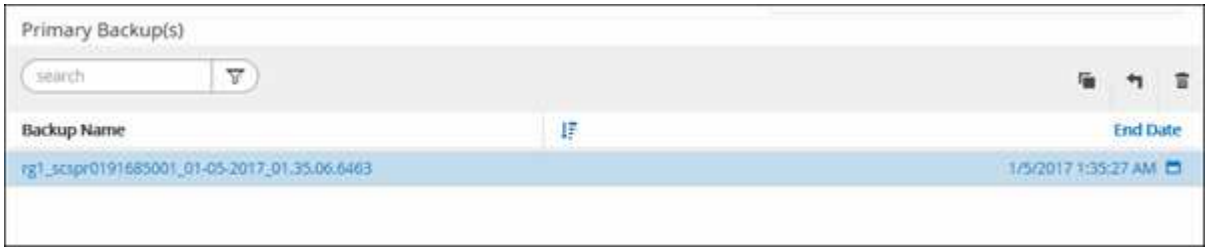
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite Wiederherstellungsbereich die Option **komplette 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 nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch 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 vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Stellen Sie ein automatisch ermittelte Datenbank-Backup wieder her

Mit SnapCenter können Daten von einem oder mehreren Backups wiederhergestellt werden.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die Sie wiederherstellen möchten.
- Für Befehle vor der Wiederherstellung, nach der Wiederherstellung, nach dem Einhängen und vor dem unmounten sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host aus den folgenden Pfaden vorhanden sind:

- 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl.

Über diese Aufgabe

- Für automatisch erkannte Ressourcen wird die Wiederherstellung mit SFSR unterstützt.
- Die automatische Point-in-Time- und Up-to-Minute-Wiederherstellung wird nicht unterstützt.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Typ, Host, zugehörigen Ressourcengruppen und -Richtlinien sowie dem Status angezeigt.

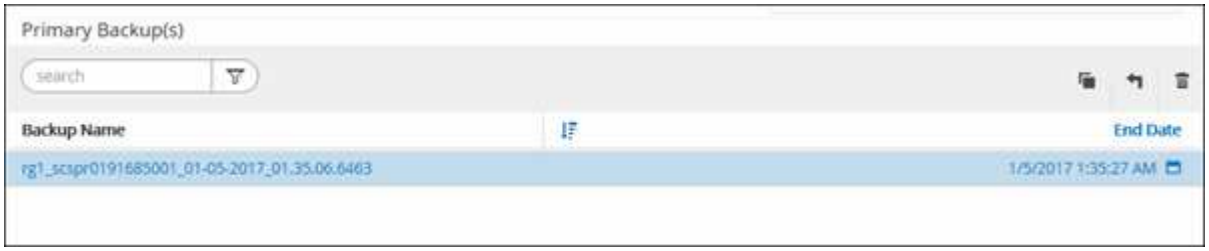
   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

   Wenn die Ressource nicht geschützt ist, wird „`not protected`“ in der Spalte Gesamtstatus angezeigt. Dies kann entweder bedeuten, dass die Ressource nicht geschützt ist oder dass die Ressource durch einen anderen Benutzer gesichert wurde.

3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * * .



6. Wählen Sie auf der Seite Wiederherstellungsumfang die Option **komplette Ressource** aus, um die konfigurierten Datenvolumes der MySQL-Datenbank wiederherzustellen.

7. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.

   Unmount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

8. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.

   Mount-Befehle sind für automatisch erkannte Ressourcen nicht verfügbar.

9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen von MySQL-Wiederherstellungsvorgängen

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung

- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Klonen von MySQL-Ressourcen-Backups

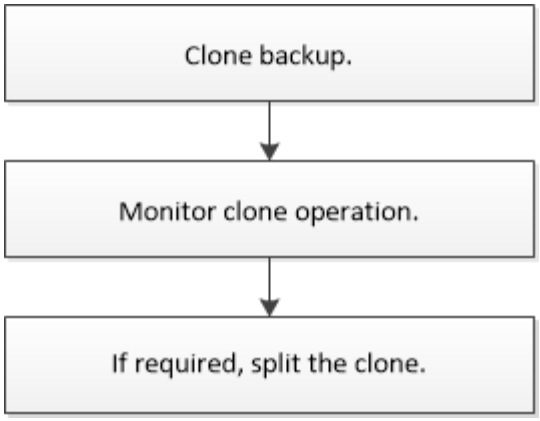
Klon-Workflow

Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

- Sie können auf dem MySQL-Quellserver klonen.
- Sie können Ressourcen-Backups aus den folgenden Gründen klonen:
  - Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
  - Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses
  - Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten detaillierte Informationen zu PowerShell Cmdlets.

Klonen eines MySQL-Backups

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen.

Bevor Sie beginnen

- Sie sollten die Ressourcen oder Ressourcengruppe gesichert haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Wenn Sie Befehle vor dem Klonen oder nach dem Klonen ausführen, sollten Sie überprüfen, ob die Befehle in der Befehlsliste auf dem Plug-in-Host über folgende Pfade vorhanden sind:
  - 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 in der Befehlsliste nicht vorhanden sind, schlägt der Vorgang fehl. * Für MySQL 5.7 sollten Sie IGNORE_MYSQLX_PORT = true (standardmäßig false) in MySQL setzen. Eigenschaftendatei.

Über diese Aufgabe

- Sie können die geklonten MySQL Instanzen nicht schützen.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Bei ONTAP 9.12.1 und älteren Versionen übernehmen die aus den SnapLock Vault Snapshots im Rahmen der Wiederherstellung erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host, zugeordnete 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 Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie einen Host aus, auf dem der Klon erstellt werden soll.
Port	Geben Sie den Port an, auf dem die geklonte MySQL-Instanz gestartet werden soll.
NFS-Export-IP-Adresse	Geben Sie IP-Adressen oder Hostnamen ein, auf denen 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 den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
      - Befehl Pre Clone: Löschen Sie vorhandene Datenbanken mit demselben Namen
      - Befehl nach Clone: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.
   b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

      Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:

   Beispiel für NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Rufen Sie die Backups für den Klonvorgang mit dem Cmdlet Get-SmBackup ab.

   Dieses Beispiel zeigt, dass zwei Backups 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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup und geben Sie die NFS-Export-IP-Adressen an, auf die die geklonten Volumes exportiert werden.

   Dieses Beispiel zeigt, dass das zu klonende Backup über eine NFSExportIPs-Adresse 10.32.212.14 verfügt:

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName
"scs000211748_gdl_englab_netapp_com_MySQL_mysqld_3306_scs000211748_0
6-26-2024_06.08.35.4307" -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306"}
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```

   Wenn NFSExportIPs nicht angegeben sind, wird der Standardwert auf den Klon-Zielhost exportiert.

4. Überprüfen Sie, ob die Backups erfolgreich geklont wurden, indem Sie das Cmdlet "Get-

SmCloneReport" verwenden, um die Details zu den Klonjobs anzuzeigen.

Sie können Details wie Klon-ID, Startdatum und -Zeit, Enddatum und -Zeit 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 Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Teilen Sie einen Klon auf

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon ist unabhängig von der übergeordneten Ressource.

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** die entsprechende Option aus der Liste Ansicht aus:

Option	Beschreibung
Für Datenbankapplikationen	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Für File-Systeme	Wählen Sie in der Liste Ansicht **Pfad** aus.

3. Wählen Sie die entsprechende Ressource aus der Liste aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Clone-Splitvorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet "Stop-SmJob" ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragzeit benötigen, um zu prüfen, ob der Klon geteilt ist oder nicht, können Sie den Wert von *CloneSplitStatusCheckPollTime* Parameter in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Clone Split-Vorgangs angezeigt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klontrennung schlägt fehl, wenn gerade Backup-, Wiederherstellungs- oder andere Klonsplitonen durchgeführt werden. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Verwandte Informationen

"Der SnapCenter Klon oder die Überprüfung schlägt fehl, wenn das Aggregat nicht vorhanden ist"

Löschen oder teilen Sie MySQL-Datenbankklone nach dem Upgrade von SnapCenter

Nach einem Upgrade auf SnapCenter 4.3 werden die Klone nicht mehr angezeigt. Sie können den Klon löschen oder die Klone auf der Topologieseite der Ressource, aus der die Klone erstellt wurden, aufteilen.

Über diese Aufgabe

Wenn Sie den Storage-Footprint der verborgenen Klone ermitteln möchten, führen Sie den folgenden Befehl aus: `Get-SmClone -ListStorageFootprint`

Schritte

1. Löschen Sie die Backups der geklonten Ressourcen mit dem Cmdlet "remove-smbackup".
2. Löschen Sie die Ressourcengruppe der geklonten Ressourcen mit dem Cmdlet "remove-sresourcgruppe".
3. Entfernen Sie den Schutz der geklonten Ressource mit dem Cmdlet "remove-smprotectResource".
4. Wählen Sie auf der Seite Ressourcen die übergeordnete Ressource aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

5. Wählen Sie in der Ansicht Kopien managen die Klone entweder auf den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen 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 Applikationen mit von NetApp unterstützten Plug-ins

Von NetApp unterstützte Plug-ins

Übersicht über die unterstützten Plug-ins von NetApp

Für Applikationen, die Sie nutzen und dann SnapCenter zum Backup, zur Wiederherstellung oder Klonen dieser Applikationen verwenden, können Sie die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und Storage Plug-in verwenden. Ihre von NetApp unterstützten Plug-ins fungieren als Host-seitige Komponenten der NetApp SnapCenter Software und ermöglichen so applikationsgerechte Datensicherung und das Management von Ressourcen.

Bei der Installation von NetApp unterstützten Plug-ins können SnapCenter mit NetApp SnapMirror Technologie genutzt werden, um Spiegelkopien von Backup Sets auf einem anderen Volume zu erstellen, und mithilfe der NetApp SnapVault Technologie Disk-to-Disk Backup-Replizierung durchzuführen. Von NetApp unterstützte Plug-ins können sowohl in Windows- als auch in Linux-Umgebungen verwendet werden.

SnapCenterCLI unterstützt keine von NetApp unterstützten Plug-ins-Befehle.

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."

Funktionen der von NetApp unterstützten Plug-ins

Sie können die von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB und Storage Plug-in für Datensicherungsvorgänge verwenden.

- Fügen Sie Ressourcen wie Datenbanken, Instanzen, Dokumente oder Tabellen hinzu.
- Backups erstellen.
- Restore aus Backups:
- Backups klonen.
- Planen von Backup-Vorgängen
- Monitoring von Backup-, Restore- und Klonvorgängen
- Berichte für Backup-, Wiederherstellungs- und Klonvorgänge anzeigen

Sie können die von NetApp unterstützten Plug-ins für Datensicherungsvorgänge verwenden.

- Erstellen Sie Konsistenzgruppen-Snapshots der Storage-Volumes über ONTAP-Cluster hinweg.
- Führen Sie Backups individueller Applikationen mithilfe des integrierten Pre- und Post-Scripting Frameworks durch

  Sie können ein Backup für das ONTAP Volume, die LUN oder einen qtree erstellen.

- Aktualisierung von Snapshots, die von Primärdaten auf eine sekundäre ONTAP erstellt wurden, mithilfe der SnapCenter Richtlinie zur Nutzung der bestehenden Replizierungsbeziehung (SnapVault/SnapMirror/einheitliche Replizierung)

  Primäre und sekundäre ONTAP können ONTAP FAS, AFF, All-SAN-Array (ASA), Select oder Cloud ONTAP sein.

- Stellen Sie komplette ONTAP Volumes, LUNs oder Dateien wieder her.

  Sie sollten den entsprechenden Dateipfad manuell angeben, da die Funktionen zum Durchsuchen oder zur Indizierung nicht im Produkt integriert sind.

  Die Wiederherstellung von qtree oder Verzeichnissen wird nicht unterstützt, aber Sie können nur den Qtree klonen und exportieren, wenn der Backup-Umfang auf Qtree-Ebene definiert ist.

Von NetApp unterstützte Plug-ins-Funktionen

SnapCenter lässt sich in die Plug-in-Applikation und mit NetApp Technologien auf dem Storage-System integrieren. Für den Einsatz mit von NetApp unterstützten Plug-ins wie MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB und Storage Plug-in nutzen Sie die grafische Benutzeroberfläche von SnapCenter.

- **Einheitliche grafische Benutzeroberfläche**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die SnapCenter Schnittstelle ermöglicht konsistente Backup-, Restore-, Recovery- und Klonvorgänge über alle Plug-ins hinweg, zentralisierte Berichterstellung, Dashboard-Ansichten auf einen Blick, rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) und das Monitoring von Aufgaben über alle Plug-ins hinweg.

- **Automatisierte zentrale Verwaltung**

  Sie können Backup-Vorgänge planen, richtlinienbasierte Backup-Aufbewahrung konfigurieren und Restore-Vorgänge durchführen. Zudem lässt sich die Umgebung proaktiv überwachen, indem SnapCenter für das Senden von E-Mail-Warnmeldungen konfiguriert wird.

- **Unterbrechungsfreie NetApp Snapshots**

  SnapCenter nutzt NetApp Snapshot Technologie mit von NetApp unterstützten Plug-ins, um Ressourcen zu sichern. Snapshots belegen nur minimalen Speicherplatz.

Die von NetApp unterstützten Plug-ins bieten darüber hinaus folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation

  Sie können die Anmeldeinformationen auch so festlegen, dass die autorisierten SnapCenter-Benutzer über Berechtigungen auf Anwendungsebene verfügen.

- Erstellung platzsparender und zeitpunktgenauer Kopien von Ressourcen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

  Auf dem Storage-System, auf dem Sie den Klon erstellen möchten, ist eine FlexClone Lizenz erforderlich.

- Unterstützung der Snapshot-Funktion von ONTAP für Konsistenzgruppen (CG) beim Erstellen von Backups.
- Fähigkeit, mehrere Backups gleichzeitig über mehrere Ressourcen-Hosts auszuführen

  In einem einzigen Vorgang werden Snapshots konsolidiert, wenn Ressourcen in einem einzelnen Host dasselbe Volume gemeinsam nutzen.

- Fähigkeit zum Erstellen von Snapshots mit externen Befehlen.
- Möglichkeit zur Erstellung Filesystem-konsistenter Snapshots in Windows Umgebungen.

Von von NetApp unterstützte Plug-ins unterstützte Storage-Typen

SnapCenter unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf Virtual Machines. Sie müssen die Unterstützung für Ihren Speichertyp überprüfen, bevor Sie von NetApp unterstützte Plug-ins installieren.

Maschine	Storage-Typ
Physische und NFS-direkte Mounts auf den VM Hosts (VMDKs und RDM LUNs werden nicht unterstützt.)	FC-verbundene LUNs
Physische und NFS-direkte Mounts auf den VM Hosts (VMDKs und RDM LUNs werden nicht unterstützt.)	ISCSI-verbundene LUNs
Physische und NFS-direkte Mounts auf den VM Hosts (VMDKs und RDM LUNs werden nicht unterstützt.)	Volumes mit NFS-Anbindung
VMware ESXi	VVol Datastores auf NFS und SAN VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.

Minimale ONTAP-Berechtigungen für von NetApp unterstütztes Plug-in erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

- Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
  - Event Generate-AutoSupport-log
  - Job-Verlauf wird angezeigt
  - Job beenden
  - lun-Attribut anzeigen
  - lun erstellen
  - lun löschen
  - lun-Geometrie
  - lun Initiatorgruppe hinzufügen

- lun-Initiatorgruppe wird erstellt
- lun-Initiatorgruppe löschen
- lun igroup umbenennen
- lun-Initiatorgruppe wird angezeigt
- lun Mapping Add-Reporting-Nodes
- lun-Zuordnung erstellen
- lun-Zuordnung löschen
- lun Mapping remove-Reporting-Nodes
- lun-Zuordnung wird angezeigt
- lun ändern
- lun-Verschiebung in Volume
- lun ist offline
- lun ist online
- die lun-Größe wird geändert
- lun seriell
- lun anzeigen
- Netzwerkschnittstelle
- SnapMirror Richtlinie Add-Rule
- änderungsregel für snapmirror
- Remove-Rule für snapmirror-Richtlinie
- snapmirror-Richtlinie anzeigen
- snapmirror Wiederherstellung
- snapmirror zeigen
- snapmirror Vorgeschichte
- snapmirror Update
- snapmirror Update-ls-Set
- snapmirror Listenziele
- Version
- Erstellung von Volume-Klonen
- Klon von Volume anzeigen
- Split-Start des Volume-Klons
- Split-Stopp für Volume-Klon
- Volume erstellen
- Volume destroy
- Erstellen eines Volume-Dateiklonen
- Show-Disk-Nutzung für Volume-Dateien
- Volume ist offline

    - Das Volume ist online
    - Volume-Änderung
    - Erstellen von Volume-qtree
    - Volume qtree löschen
    - Änderung des Volume-qtree
    - Volume-qtree anzeigen
    - Volume-Einschränkung
    - Volumen anzeigen
    - Erstellen von Volume-Snapshots
    - Volume Snapshot löschen
    - Ändern des Volume-Snapshots
    - Umbenennung von Volume-Snapshots
    - Wiederherstellung von Volume Snapshots
    - Restore-Datei für Volume Snapshots
    - Volume-Snapshot werden angezeigt
    - Volume-Aufhängung nicht verfügbar
    - cifs von vserver
    - erstellung von cifs-Freigaben von vserver
    - cifs-Freigabe von vserver: Löschen
    - vserver cifs shadowcopy anzeigen
    - cifs-Freigabe von vserver wird angezeigt
    - vserver cifs zeigen
    - Erstellung von vserver Exportrichtlinien
    - vserver: Löschen der Exportrichtlinie
    - Erstellung von vserver Export-Policy-Regel
    - vserver: Export-Policy-Regel anzeigen
    - vserver Export-Policy wird angezeigt
    - vserver iscsi-Verbindung wird angezeigt
    - vserver zeigen
- Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
    - Netzwerkschnittstelle

Vorbereiten der Storage-Systeme für die SnapMirror und SnapVault Replizierung für von NetApp unterstützte Plug-ins

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese

Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates für SnapMirror und SnapVault durch, nachdem der Snapshot Vorgang abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primary** > **Mirror** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror Beziehungen und deren Einrichtung finden Sie unter "ONTAP-Dokumentation".

Backup-Strategie definieren

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backup-Jobs erstellen, stellen Sie sicher, dass Sie über die Backups verfügen, die Sie benötigen, um Ihre Ressourcen erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Über diese Aufgabe

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Schritte

1. Bestimmen Sie, wann die Ressourcen gesichert werden sollen.
2. Legen Sie fest, wie viele Backup-Jobs Sie benötigen.
3. Geben Sie an, wie Sie Ihre Backups benennen.
4. Legen Sie fest, ob Sie Snapshots von Konsistenzgruppen erstellen möchten, und entscheiden Sie sich für die entsprechenden Optionen zum Löschen von Snapshots von Konsistenzgruppen.
5. Entscheiden Sie, ob Sie NetApp SnapMirror Technologie zur Replizierung oder NetApp SnapVault Technologie zur langfristigen Aufbewahrung verwenden möchten.
6. Bestimmen Sie den Aufbewahrungszeitraum für die Snapshots auf dem Quell-Storage-System und dem SnapMirror Ziel.

7. Bestimmen Sie, ob Sie vor oder nach dem Backup Befehle ausführen möchten, und geben Sie ein Prescript oder ein Postscript an.

Backup-Strategie für von NetApp unterstützte Plug-ins

Backup-Pläne von von NetApp unterstützten Plug-in-Ressourcen

Der wichtigste Faktor beim Bestimmen eines Backup-Zeitplans ist die Änderungsrate für die Ressource. Je öfter Sie Ihre Ressourcen sichern, desto weniger Archivprotokolle, die SnapCenter für die Wiederherstellung verwenden muss, was zu schnelleren Restore-Vorgängen führen kann.

Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, die Service Level Agreement (SLA) und den Recovery Point Objective (RPO).

Im Rahmen des SLA wird das erwartete Service-Level definiert und es werden zahlreiche Service-bezogene Probleme behandelt, darunter Verfügbarkeit und Performance des Service. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

  Die Backup-Frequenz (wie oft Backups durchgeführt werden sollen), auch als Zeitplantyp für einige Plug-ins bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können z. B. die Backup-Häufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren. Über die SnapCenter-Benutzeroberfläche können Sie auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressource oder Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan für die Sicherung jeden Donnerstag um 10:00 Uhr konfigurieren. Sie können auf die Zeitpläne für Ressourcengruppen in der SnapCenter-Benutzeroberfläche zugreifen, indem Sie auf **Ressourcen** klicken und dann das entsprechende Plug-in auswählen. und klicken Sie auf **Ansicht** > **Ressourcengruppe**.

Anzahl der erforderlichen Backup-Jobs

Zu den Faktoren, die die Anzahl der erforderlichen Backup-Jobs bestimmen, zählen die Größe der Ressource, die Anzahl der verwendeten Volumes, die Änderungsrate der Ressource und Ihr Service Level Agreement (SLA).

Die Anzahl der ausgewählten Backup-Jobs hängt in der Regel von der Anzahl der Volumes ab, von denen Sie Ihre Ressourcen platziert haben. Wenn Sie beispielsweise eine Gruppe kleiner Ressourcen auf einem Volume und einer großen Ressource auf einem anderen Volume platziert haben, können Sie für die kleinen Ressourcen einen Backup-Job und für die große Ressource einen Backup-Job erstellen.

Typen von Wiederherstellungsstrategien, die für manuell hinzugefügte NetApp-unterstützte Plug-in-Ressourcen unterstützt werden

Sie müssen eine Strategie definieren, bevor Sie die Restore-Vorgänge 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.

Komplette Ressourcenwiederherstellung

- Stellt alle Volumes, qtrees und LUNs einer Ressource wieder her

Wenn die Ressource Volumes oder qtrees enthält, werden die nach dem ausgewählten Snapshot für die Wiederherstellung auf diesen Volumes oder qtrees erstellten Snapshots gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf den gleichen Volumes oder qtrees gehostet wird, wird diese Ressource auch gelöscht.

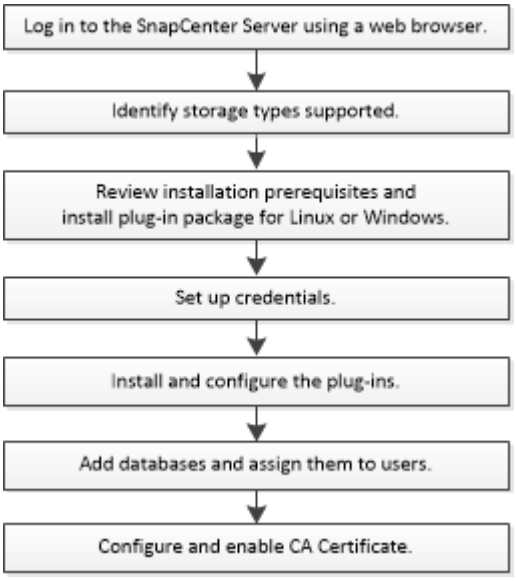
Wiederherstellung auf Dateiebene

- Wiederherstellung von Dateien aus Volumes, qtrees oder Verzeichnissen
- Stellt nur die ausgewählten LUNs wieder her

Bereiten Sie die Installation von NetApp-unterstützten Plug-ins vor

Installations-Workflow von von SnapCenter NetApp unterstützten Plug-ins

Sie sollten von SnapCenter NetApp unterstützte Plug-ins installieren und einrichten, wenn Sie die von NetApp unterstützten Plug-in-Ressourcen schützen möchten.



Voraussetzungen für das Hinzufügen von Hosts und das Installieren des Plug-ins-Pakets für Windows, Linux oder AIX

Bevor Sie einen Host hinzufügen und die Plug-ins-Pakete installieren, müssen Sie alle Anforderungen erfüllen. Von NetApp unterstützte Plug-ins werden auf Windows-, Linux- und AIX-Umgebungen unterstützt.

Storage und Oracle Applikationen werden auf AIX unterstützt.

- Sie müssen Java 11 auf Ihrem Linux-, Windows- oder AIX-Host installiert haben.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC 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 zur Verfügung stehen, von dem aus der Host-Zusatzvorgang ausgeführt wird.

Allgemein

Wenn Sie iSCSI verwenden, sollte der iSCSI-Dienst ausgeführt werden.

Windows Hosts

- Sie müssen über einen Domänenbenutzer mit lokalen Administratorrechten mit lokalen Anmeldeberechtigungen auf dem Remote-Host verfügen.
- Wenn Sie Cluster-Nodes in SnapCenter verwalten, müssen Sie einen Benutzer mit Administratorrechten für alle Nodes im Cluster besitzen.
- Sie müssen manuell das SnapCenter-Plug-in für Microsoft Windows auswählen.

Linux- und AIX-Hosts

Storage und Oracle Applikationen werden auf 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 Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu Anforderungen.

  "Java-Downloads für alle Betriebssysteme"

  "NetApp Interoperabilitäts-Matrix-Tool"

- Sie müssen sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um Zugriff auf mehrere Pfade zu ermöglichen. Fügen Sie die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

AIX Host-Anforderungen

Bevor Sie das SnapCenter Plug-ins Package für AIX installieren, sollten Sie sicherstellen, dass der Host die Anforderungen erfüllt.

Storage und Oracle Applikationen werden auf AIX unterstützt.

Das SnapCenter Plug-in für UNIX, das Teil des SnapCenter Plug-ins-Pakets für AIX ist, unterstützt keine gleichzeitigen Volume-Gruppen.

Element	Anforderungen
Betriebssysteme	AIX 7.1 oder höher
MindestRAM für das SnapCenter Plug-in auf dem Host	4GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 IBM Java Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Konfigurieren Sie sudo-Berechtigungen für Benutzer, die nicht root sind, für 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 Authentifizierungscode Macs hmac-sha2-256 und MACs hmac-sha2-512 zu konfigurieren.

  Starten Sie den sshd-Dienst nach dem Aktualisieren 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 ermöglichen:

- /Home/*AIX_USER*/.sc_netapp/snapcenter_aix_Host_Plugin.bsx
- /Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/Deinstallation
- /Custom_location/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 die folgenden Zeilen zur Datei /etc/sudoers mit dem Dienstprogramm visudo Linux 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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Wenn Sie über ein RAC Setup verfügen, und die anderen zulässigen Befehle, sollten Sie die Datei /etc/sudoers: '/<crs_home>/bin/olsnodes' hinzufügen.

Sie können den Wert von *crs_Home* aus der Datei */etc/oracle/olr.loc* erhalten.

AIX_USER ist der Name des nicht-root-Benutzers, den Sie erstellt haben.

Sie können die Datei *Checksumme_value* aus der Datei **sc_unix_Plugins_Checksumme.txt** abrufen, die sich unter folgender Adresse befindet:

- *C:\ProgramData\NetApp\SnapCenter\Paket-Repository\sc_unix_Plugins_Checksumme.txt* wenn SnapCenter-Server auf Windows-Host installiert ist.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_Plugins_checksum.txt* wenn SnapCenter-Server auf Linux-Host installiert ist.

Das Beispiel sollte nur als Referenz zur Erstellung eigener Daten verwendet werden.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• .NET Core beginnt mit Version 8.0.5 und enthält alle nachfolgenden .NET 8-Patches • PowerShell Core 7.4.2 • Java 11 Oracle Java und OpenJDK Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Für . Informationen zur NETZSPEZIFISCHEN Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

Host-Anforderungen für die Installation des SnapCenter-Plug-ins-Pakets für Linux und AIX

Stellen Sie sicher, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX installieren.

Storage und Oracle Applikationen werden auf AIX unterstützt.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
MindestRAM für das SnapCenter Plug-in auf dem Host	1GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java oder OpenJDK Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool"

Richten Sie Anmeldeinformationen für von NetApp unterstützte Plug-ins ein

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren. Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datenschutzvorgängen in 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 Anmeldedaten für den Root-Benutzer oder für einen Benutzer ohne Root einrichten, der über sudo-Berechtigungen verfügt, um das Plug-in zu installieren und zu starten.

  Best Practice: Obwohl Sie nach der Bereitstellung von Hosts und der Installation von Plug-ins Anmeldedaten für Linux erstellen dürfen, empfiehlt es sich, nach dem Hinzufügen von SVMs Anmeldeinformationen 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 Anmeldedaten mit Administratorrechten einrichten, einschließlich Administratorrechten auf dem Remote-Host.

- Von NetApp unterstützte Plug-ins-Applikationen

  Das Plug-in verwendet die Anmeldeinformationen, die beim Hinzufügen einer Ressource ausgewählt oder erstellt wurden. Wenn eine Ressource während des Datenschutzvorgangs keine Anmeldeinformationen benötigt, können Sie die Anmeldeinformationen auf **Keine** setzen.

Über diese Aufgabe

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite **Credential** die Informationen an, die zum Konfigurieren von Anmeldeinformationen erforderlich sind:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten ein.

Für dieses Feld…	Tun Sie das…
Benutzername	Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung verwendet werden sollen. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind: ◦ *NetBIOS\Benutzername* ◦ *Domain FQDN\Benutzername* • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet: *Username*
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, den Sie verwenden möchten.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen **Sudo-Berechtigungen verwenden**, wenn Sie Anmeldedaten für einen nicht-Root-Benutzer erstellen möchten. Gilt nur für Linux- und AIX-Benutzer.

5. Klicken Sie auf **OK**.

Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie einem Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung der Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Bevor Sie beginnen

- Sie sollten einen Windows Server 2016 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2016 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Beispiel:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Führen Sie den Befehl aus `Get-ADServiceAccount` , um das
Dienstkonto zu überprüfen.
```

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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

b. Installieren Sie gMSA auf Ihrem Host, indem Sie den folgenden Befehl über die 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 Service-Login-Konto verwendet.

Installieren Sie die von NetApp unterstützten Plug-ins

Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts

Sie müssen die Seite SnapCenter Host hinzufügen verwenden, um Hosts hinzuzufügen, und dann die Plug-in-Pakete 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, der einer Rolle zugewiesen wird, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter Admin“.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange ausgeführt wird.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

"Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2016 oder höher für benutzerdefinierte Anwendungen"

- Für Windows-Host müssen Sie sicherstellen, dass Sie SnapCenter-Plug-in für Windows auswählen.

Über diese Aufgabe

- 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 Nodes des Clusters installiert.

Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ aus: • Windows • Linux • AIX Die von NetApp unterstützten Plug-ins können in Windows-, Linux- und AIX-Umgebungen verwendet werden. Storage und Oracle Applikationen werden auf AIX unterstützt.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. In Windows-Umgebungen wird die IP-Adresse nur für nicht vertrauenswürdige Domänen-Hosts unterstützt, wenn sie in den FQDN auflöst. Sie können die IP-Adressen oder FQDN eines eigenständigen Hosts eingeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus, oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt **Plug-ins zur Installation auswählen** die zu installierenden Plug-ins aus.

   Sie können die folgenden Plug-ins aus der Liste installieren:

   - MongoDB
   - ORASCPM (angezeigt als Oracle Applications)
   - SAP ASE
   - SAP MaxDB
   - Storage

6. (Optional) Wählen Sie **Weitere Optionen**, um die anderen Plug-ins zu installieren.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Die von NetApp unterstützten Plug-ins können entweder auf einem Windows-System oder auf einem Linux-System installiert werden. • Der Standardpfad für das SnapCenter Plug-ins-Paket für Windows ist C:\Programme\NetApp\SnapCenter. Optional können Sie den Pfad anpassen. • Für SnapCenter Plug-ins Paket für Linux und SnapCenter Plug-ins Paket für AIX ist der Standardpfad `/opt/NetApp/snapcenter` . Optional können Sie den Pfad anpassen.
Überspringen Sie die Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

Für dieses Feld…	Tun Sie das…
Verwenden Sie Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie für Windows-Host dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: Domainname\AccountName€. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Wählen Sie **Senden**.

   Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, RAM, PowerShell-Version, . NET-Version, Speicherort (für Windows-Plug-ins) und Java-Version (für Linux-Plug-ins) werden mit den Mindestanforderungen validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

   Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei Web.config unter aktualisieren `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 lautet `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

   Der Standardpfad für Linux lautet `/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**.

   Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Protokolldateien befinden sich in `/custom_location/snapcenter/` Logs.

Installieren Sie mithilfe von Cmdlets SnapCenter-Plug-in-Pakete für Linux, Windows oder AIX auf mehreren Remote-Hosts

Sie können die SnapCenter-Plug-in-Pakete für Linux, Windows oder AIX gleichzeitig auf mehreren Hosts installieren, indem Sie das Cmdlet "Install-SmHostPackage PowerShell" verwenden.

Bevor Sie beginnen

Der Benutzer, der einen Host hinzugefügt hat, sollte über die Administratorrechte auf dem Host verfügen.

Storage und Oracle Applikationen werden auf AIX unterstützt.

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet "Open-SmConnection" und geben Sie dann Ihre Anmeldeinformationen ein.
3. Installieren Sie das Plug-in auf mehreren Hosts mit dem Cmdlet "Install-SmHostPackage" und den erforderlichen Parametern.

   Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

   Sie können die Option -skipprecheck verwenden, wenn Sie die Plug-ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen erfüllt, um das Plug-in zu installieren.

4. Geben Sie Ihre Anmeldeinformationen für die Remote-Installation ein.

Installieren Sie die von NetApp unterstützten Plug-ins auf Linux Hosts über die Befehlszeilenschnittstelle

Sie sollten die von NetApp unterstützten Plug-ins über die SnapCenter-Benutzeroberfläche (UI) installieren. Wenn Ihre Umgebung die Remote-Installation des Plug-ins über die SnapCenter-Benutzeroberfläche nicht zulässt, können Sie die von NetApp unterstützten Plug-ins entweder im Konsolenmodus oder im unbeaufsichtigten Modus über die Befehlszeilenschnittstelle (CLI) installieren.

Schritte

1. Kopieren Sie die Installationsdatei für das SnapCenter-Plug-ins-Paket für Linux (snapcenter_linux_Host_Plugin.bin) von C:\ProgramData\NetApp\SnapCenter\Paketrepository auf den Host, auf dem Sie die von NetApp unterstützten Plug-ins installieren möchten.

   Sie können von dem Host, auf dem der SnapCenter-Server installiert ist, auf diesen Pfad zugreifen.

2. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem 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 HTTPS-Kommunikationsport SMCore 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 das SnapCenter-Plug-ins-Paket für Linux installiert werden soll.
- _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.

   Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

5. Melden Sie sich bei SnapCenter an und laden Sie das von NetApp unterstützte Plug-in über die UI oder mithilfe von PowerShell Cmdlets hoch.

   Sie können das von NetApp unterstützte Plug-in über die Benutzeroberfläche hochladen, indem Sie den "Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts" Abschnitt verwenden.

   Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets.

   "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen Sie den Status der Installation von NetApp-unterstützten Plug-ins

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden, gehen Sie wie folgt vor:
   a. Klicken Sie Auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

DIE Länge des RSA-Schlüssels des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CSR-Datei für das CA-Zertifikat".

Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie das Feld Alternative Name (SAN) des Studienteilnehmers ausfüllen, bevor Sie das Zertifikat beschaffen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf

Hinzufügen.

3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Import**, um den Importassistenten zu starten.
6. Füllen Sie den Assistenten wie folgt aus:

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

      Wenn der Daumendruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, wird nach dem Entfernen der Leerzeichen der Text „a909502dd82ae41433e6f83886b00d4277a32a7b“ lauten.

2. Führen Sie Folgendes aus PowerShell aus:
    a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

       Get-ChildItem -Path Cert:\LocalMachine\My

    b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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-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.

   Es ist der Wert, der dem Schlüssel 'KEYSTORE_PASS' entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

> ⓘ 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen 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. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das Standardkennwort für den 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 Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei
agent.properties.
```

Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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 SnapCenter-Plug-Ins

Über diese Aufgabe

- 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 mit dem Schlüssel CRL_PATH ändern und aktualisieren.

   Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Konfigurieren Sie das CA-Zertifikat für den von NetApp unterstützten 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 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 ist der Wert, der dem Schlüssel *KEYSTORE_PASS* entspricht.

2. Ändern Sie das Schlüsselspeicher-Passwort:

   Keytool -storepasswd -keystore keystore.jks

Wenn der Befehl "keytool" in der Windows-Eingabeaufforderung nicht erkannt wird, ersetzen Sie den Befehl keytool mit seinem vollständigen Pfad.

C:\Programme\Java\<jdk_Version>\bin\keytool.exe“ -storepasswd -keystore keystore.jks

3. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:

   Keytool -keypasswd -alias „alias_Name_in_cert“ -keystore keystore.jks

   Aktualisieren Sie das gleiche für den Schlüssel KEYSTORE_PASS in *agent.properties* Datei.

4. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

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: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

   Keytool -list -V -keystore keystore.jks

4. Fügen Sie ein Stammzertifikat oder ein 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 Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate 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 enthält: *C:\Programme\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Suchen Sie die Datei *keystore.jks*.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

Keytool -list -V -keystore keystore.jks

4. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen 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. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält, der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt wurde.
7. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für das CA-Zertifikat in das Schlüsselspeicher-Passwort.

   Das Standardkennwort für den Plug-in-Keystore ist der Wert des Schlüssels KEYSTORE_PASS in der Datei agent.properties.

   Keytool -keypasswd -alias „alias_Name_in_CA_cert“ -keystore keystore.jks

8. Konfigurieren Sie den Alias-Namen aus dem CA-Zertifikat in der Datei *agent.properties*.

   Diesen Wert mit dem Schlüssel SCC_CERTIFICATE_ALIAS aktualisieren.

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

Über diese Aufgabe

- Die neueste CRL-Datei für das zugehörige CA-Zertifikat finden Sie unter "Aktualisieren der Listendatei für Zertifikatsperrlisten 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* mit dem Schlüssel CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Bereiten Sie sich auf die Datensicherung vor

Voraussetzungen für die Verwendung der von NetApp unterstützten Plug-ins

Bevor Sie von SnapCenter NetApp unterstützte Plug-ins verwenden, muss der SnapCenter-Administrator den SnapCenter-Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installation und Konfiguration von SnapCenter Server
- Melden Sie sich beim SnapCenter-Server an.
- Konfigurieren Sie die SnapCenter Umgebung, indem Sie Storage-Systemverbindungen hinzufügen und ggf. Anmeldedaten 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 mehrere Datenpfade (LIFs) oder eine dNFS-Konfiguration haben, können Sie Folgendes mithilfe der SnapCenter-CLI auf dem Datenbank-Host durchführen:
  - Standardmäßig werden alle IP-Adressen des Datenbank-Hosts der Richtlinie für den NFS-Storage-Export 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 in SVMs mehrere Datenpfade (LIFs) vorhanden sind, wählt SnapCenter den entsprechenden Datenpfad (LIF) zur Mounten des geklonten NFS-Volumes. Wenn Sie jedoch einen bestimmten Datenpfad (LIF) angeben möchten, müssen Sie die CLI Set-SvmPreferredDataPath ausführen. Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Command Reference Guide".

- Richten Sie SnapMirror und SnapVault ein, sofern Sie eine Backup-Replizierung möchten.
- 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.

Wie Ressourcen, Ressourcengruppen und Richtlinien zum Schutz von von NetApp unterstützten Plug-in-Ressourcen verwendet werden

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- Ressourcen sind normalerweise Datenbanken, Windows File-Systeme 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 von Ihnen für die Ressourcengruppe festgelegten Zeitplan aus.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen durchführen.

- Die Richtlinien legen die Backup-Häufigkeit, die Aufbewahrung von Kopien, die Replizierung, Skripte und andere Merkmale von Datensicherungsvorgängen fest.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf für eine einzelne Ressource durchführen.

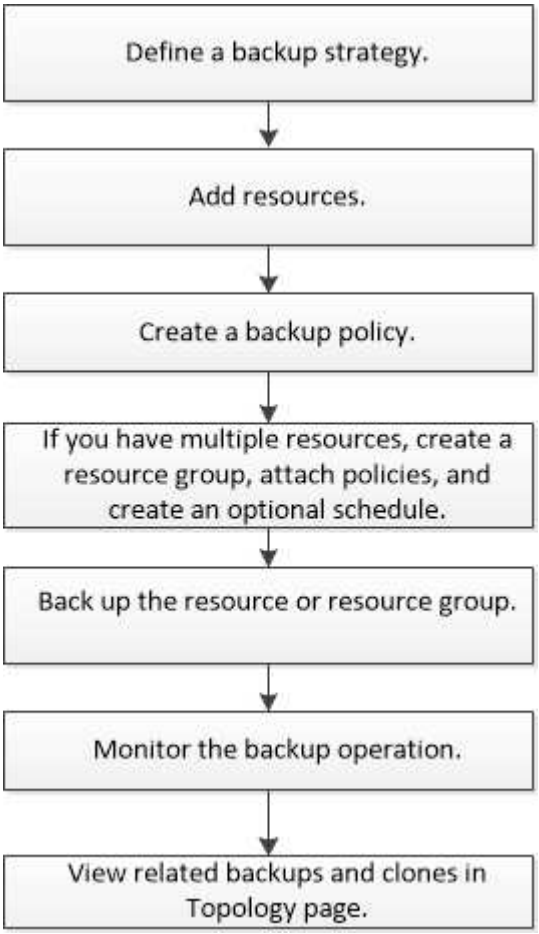
Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme des Hosts enthält. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik. Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppen so konfigurieren, dass sie täglich ein dateibasiertes Backup durchführen, und einen anderen Zeitplan, der stündliche Snapshot-basierte Backups durchführt.

Backup von von NetApp unterstützten Plug-ins-Ressourcen

Backup von von NetApp unterstützten Plug-ins-Ressourcen

Der Backup-Workflow umfasst die Planung, die Ermittlung der Backup-Ressourcen, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch"

Hinzufügen von Ressourcen zu von NetApp unterstützten Plug-ins

Sie müssen die Ressourcen hinzufügen, die Sie sichern oder klonen möchten. Je nach Umgebung können sich die Ressourcen entweder um Datenbankinstanzen oder Sammlungen handeln, die Sie sichern oder klonen möchten.

Bevor Sie beginnen

- Sie müssen Aufgaben wie das Installieren des SnapCenter-Servers, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen

abgeschlossen haben.

- Sie müssen die Plug-ins auf SnapCenter Server hochgeladen haben.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **Ressource hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails bereitstellen“ die folgenden Aktionen durch:

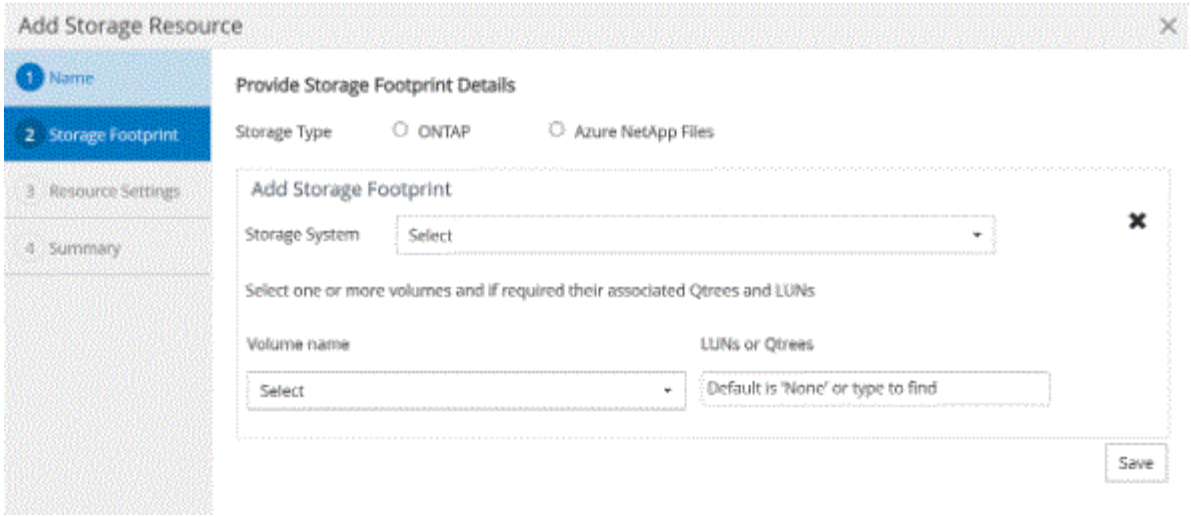
Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressource ein.
Host-Name	Wählen Sie den Host aus.
Typ	Wählen Sie den Typ aus. Der Typ ist gemäß der Plug-in-Beschreibungsdatei Benutzerdefiniert. Beispiel: Datenbank und Instanz. Wenn der ausgewählte Typ ein übergeordnetes Element hat, geben Sie die Details des übergeordneten Typs ein. Wenn der Typ beispielsweise „Datenbank“ und „übergeordnetes Objekt“ ist, geben Sie die Details der Instanz ein.
Name der Anmeldeinformationen	Wählen Sie Anmeldedaten aus oder erstellen Sie eine neue Berechtigung.
Mount-Pfade	Geben Sie die Mount-Pfade ein, auf denen die Ressource angehängt ist. Dies gilt nur für einen Windows-Host.

4. Wählen Sie auf der Seite „Speicherplatz bereitstellen“ ein Speichersystem aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und wählen Sie dann **Speichern** aus.

   Optional: Wählen Sie das Symbol aus  , um weitere Volumes, LUNs und qtrees von anderen Storage-Systemen hinzuzufügen.

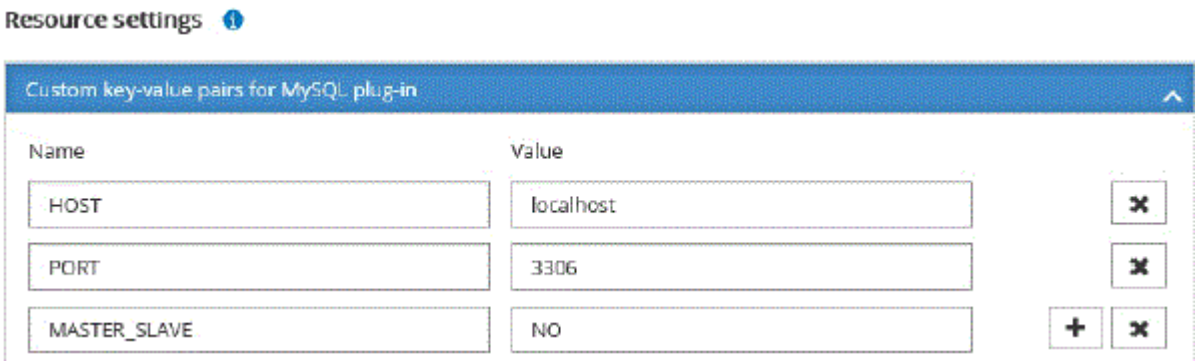
   

   Von NetApp unterstützte Plug-ins unterstützen keine automatische Erkennung der Ressourcen. Die Speicherdetails physischer und virtueller Umgebungen werden ebenfalls nicht automatisch erkannt. Sie müssen Storage-Informationen für physische und virtuelle Umgebungen bereitstellen und gleichzeitig Ressourcen erstellen.



5. Stellen Sie auf der Seite „Ressourceneinstellungen“ benutzerdefinierte Key-Value-Paare für die Ressource bereit.

   Stellen Sie sicher, dass der Name der benutzerdefinierten Schlüssel in Großbuchstaben angegeben ist.

   Informationen zu den jeweiligen Plug-in-Parametern finden Sie unter "Parameter zum Konfigurieren der Ressource"

6. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Ergebnis

Die Ressourcen werden zusammen mit Informationen wie Typ, Host- oder Cluster-Name, zugeordnete Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.

Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Nachdem Sie fertig sind

Wenn Sie anderen Benutzern Zugriff auf die Assets gewähren möchten, muss der SnapCenter-Administrator diesen Benutzern Assets zuweisen. Auf diese Weise 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-ins-Ressource Backups 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 mithilfe der folgenden Parameter auf der Seite „Ressourceneinstellungen“ konfigurieren.

Plug-in für MongoDB

Ressourceneinstellungen:

- MONGODB_APP_SERVER=(für Ressourcentyp als freigebundener Cluster) oder MONGODB_REPLICASET_SERVER=(für Ressourcentyp als Replikaset)
- OPOG_PATH=(Optionaler Parameter, falls er von MongoDB.propertiesfile bereitgestellt wird)
- MONGODB_AUTHENTICATION_TYPE= (EINFACH für LDAP-Authentifizierung und keine für andere)

Die folgenden Parameter müssen in der Datei MongoDB.properties angegeben werden:

- DISABLE_STARTING_STOPPING_SERVICES=
  - N wenn die Start/Stopp-Dienste vom Plug-in ausgeführt werden.
  - Y wenn Start-/**Stopp-Services vom Benutzer durchgeführt werden.
  - Der optionale Parameter als Standardwert ist auf N gesetzt
- OPOG_PATH_= (Optionaler Parameter, falls er bereits als benutzerdefiniertes Schlüssel-Wert-Paar in SnapCenter angegeben ist).

Plug-in für MaxDB

Ressourceneinstellungen:

- XUSER_ENABLE (J/N) aktiviert oder deaktiviert die Verwendung eines xuser für MaxDB, so dass für den Datenbankbenutzer kein Passwort erforderlich ist.
- HANDLE_LOGWRITER (J/N) führt die Operationen zum Anhalten des Logwriter (N) oder zum Fortsetzen des Logwriter (Y) aus.
- DBMCLICMD (path_to_dbmcli_cmd) gibt den Pfad zum Befehl MaxDB dbmcli an. Wenn nicht festgelegt, wird dbmcli auf dem Suchpfad verwendet.

  In Windows-Umgebungen muss sich der Pfad in doppelten Anführungszeichen („…“) befinden.

- SQLCLICMD (Path_to_sqlcli_cmd) gibt den Pfad zum MaxDB sqlcli-Befehl an. Wenn der Pfad nicht festgelegt ist, wird sqlcli auf dem Suchpfad verwendet.
- MAXDB_UPDATE_HIST_LOG (J/N) weist das MaxDB-Sicherungsprogramm an, ob es das MaxDB-Verlaufsprotokoll aktualisieren soll.
- MAXDB_CHECK_SNAPSHOT_dir : Beispiel, SID1:Directory[,Directory…]; [SID2:directoary[,Directory…] Überprüft, ob ein Snap Creator Snapshot Kopiervorgang erfolgreich war, und stellt sicher, dass der Snapshot erstellt wird.

  Dies bezieht sich nur auf NFS. Das Verzeichnis muss auf den Speicherort verweisen, der das Verzeichnis .Snapshot enthält. Mehrere Verzeichnisse können in eine kommagetrennte Liste aufgenommen werden.

  In MaxDB 7.8 und neueren Versionen ist die Datenbank-Backup-Anforderung im Backup-Verlauf als fehlgeschlagen markiert.

- MAXDB_BACKUP_TEMPLATES: Gibt eine Backup-Vorlage für jede Datenbank an.

  Die Vorlage muss vorhanden sein und eine externe Art von Backup-Vorlage sein. Um die Snapshot-Integration für MaxDB 7.8 und höher zu ermöglichen, müssen Sie über die Funktionalität des MaxDB Hintergrundservers verfügen und die MaxDB Backup-Vorlage des EXTERNEN Typs bereits konfiguriert haben.

- MAXDB_BG_SERVER_PREFIX: Gibt das Präfix für den Namen des Hintergrundservers 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 (-S Option auf isql-Befehl). Beispiel: P_Test.
- SYBASE_DATABASES_EXCLUDE (db_Name) ermöglicht es, Datenbanken auszuschließen, wenn das Konstrukt „ALL“ verwendet wird.

  Sie können mehrere Datenbanken mithilfe einer durch Semikolon getrennten Liste angeben. 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 Stopp-Befehle von 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, für die ein Transaktions-Dump erforderlich ist.

- SYBASE_TRAN_DUMP_COMPRESS (J/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 (J/N) können Sie benutzerdefinierte temporäre Datenbanken automatisch ausschließen.

Plug-in für Oracle Applications (ORASCPM)

Ressourceneinstellungen:

- SQLPLUS_CMD gibt den Pfad zu sqlplus an.
- ORACLE_DATABASES listet die zu sichernden Oracle-Datenbanken und den entsprechenden Benutzer (Database:User) 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 beim Ausführen von */bin/su <Benutzer, der sqlplus ausführt> -c sqlplus /nolog <Befehl>* erneut exportiert werden sollen. Dies ist typischerweise der Fall, wenn der Benutzer, der sqlplus ausführt, nicht alle Umgebungsvariablen gesetzt hat, die für die Verbindung zur Datenbank mit *connect / as sysdba* erforderlich sind.

Erstellen von Richtlinien für von NetApp unterstützte Plug-in-Ressourcen

Bevor Sie SnapCenter zum Sichern bestimmter NetApp-unterstützter Plug-in-Ressourcen verwenden, müssen Sie eine Backup-Richtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten.

Bevor Sie beginnen

- Sie sollten Ihre Backup-Strategie definiert haben.

  Weitere Details finden Sie in den Informationen zur Definition einer Datensicherungsstrategie für von NetApp unterstützte Plug-ins.

- Sie sollten sich auf die Datensicherung vorbereiten.

  Die Vorbereitung auf die Datensicherung umfasst Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erstellen von Verbindungen zum Storage-System und das Hinzufügen von Ressourcen.

- Die Storage Virtual Machines (SVMs) sollten Ihnen für Spiegelungs- oder Vault-Vorgänge zugewiesen werden.

  Der SnapCenter Administrator muss Ihnen die SVMs sowohl für die Quell- als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren.

- Sie sollten die Ressourcen, die Sie schützen möchten, manuell hinzugefügt haben.

Über diese Aufgabe

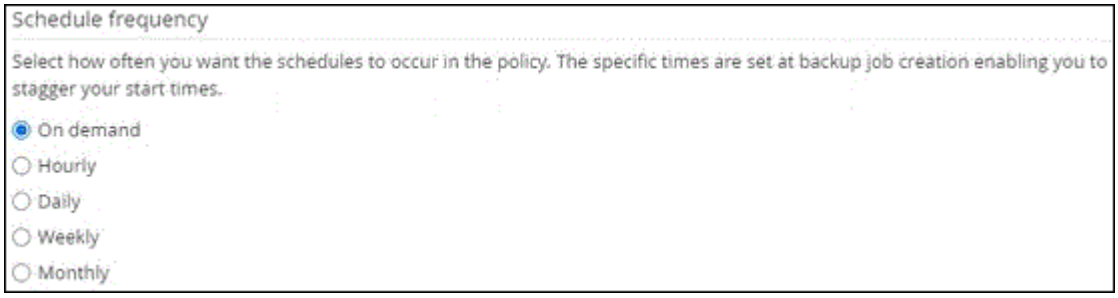
- Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln. Außerdem können Sie Replizierungs-, Skript- und Applikationseinstellungen festlegen.
- Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.
- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.
  - Wenn Sie eine Snapshot-Sperrfrist festlegen, wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.
  - Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

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 Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Einstellungen die folgenden Schritte aus:
   - Geben Sie den Terminplantyp an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

     Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

     Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

   - Geben Sie im Abschnitt Benutzerdefinierte Backup-Einstellungen alle spezifischen Backup-Einstellungen an, die an das Plug-in-in-Schlüsselwert-Format übergeben werden müssen. Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.
6. Geben Sie auf der Seite **Aufbewahrung** die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite **Sicherungstyp** ausgewählten Zeitplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Total Snapshot Copies to keep** aus, und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Snapshot-Kopien behalten für**, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots vor dem Löschen behalten möchten.
Sperrfrist von Snapshot-Kopien	Wählen Sie als Sperrzeitraum für Snapshots Tage, Monate oder Jahre aus. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

7. Geben Sie auf der Seite **Replikation** die Replikationseinstellungen an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Wenn die Sicherungsbeziehung in ONTAP vom Typ „Mirror and Vault“ ist und Sie nur diese Option auswählen, wird auf dem primären Snapshot nicht an das Zielsystem übertragen, sondern auf dem Zielsystem aufgelistet. Wenn dieser Snapshot vom Ziel ausgewählt wurde, um einen Wiederherstellungsvorgang durchzuführen, wird die folgende Fehlermeldung angezeigt: Sekundärer Speicherort ist für das ausgewählte Backup mit vaulted/mirrored nicht verfügbar. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Siehe "Zeigen Sie auf der Seite Topologie die ressourcenbezogenen Backups und Klone von NetApp-unterstützten Plug-in an".

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen. Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden. Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert. Weitere Informationen zu SnapLock Vault finden Sie unter Festsetzen von Snapshots auf WORM auf einem Vault-Ziel "Zeigen Sie auf der Seite Topologie die ressourcenbezogenen Backups und Klone von NetApp-unterstützten Plug-in an".
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. ⓘ Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Anzahl der Wiederholversuche	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Es ermöglicht Ihnen, alle Daten, die einer bestimmten Anwendung zugeordnet sind, gleichzeitig zu sichern. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Hinweis: Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, finden Sie später alle Ressourcengruppen, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll. Beispiel: *Custext_Resource Group_Policy_hostname oder Resource Group_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

4. Optional: Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und den Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

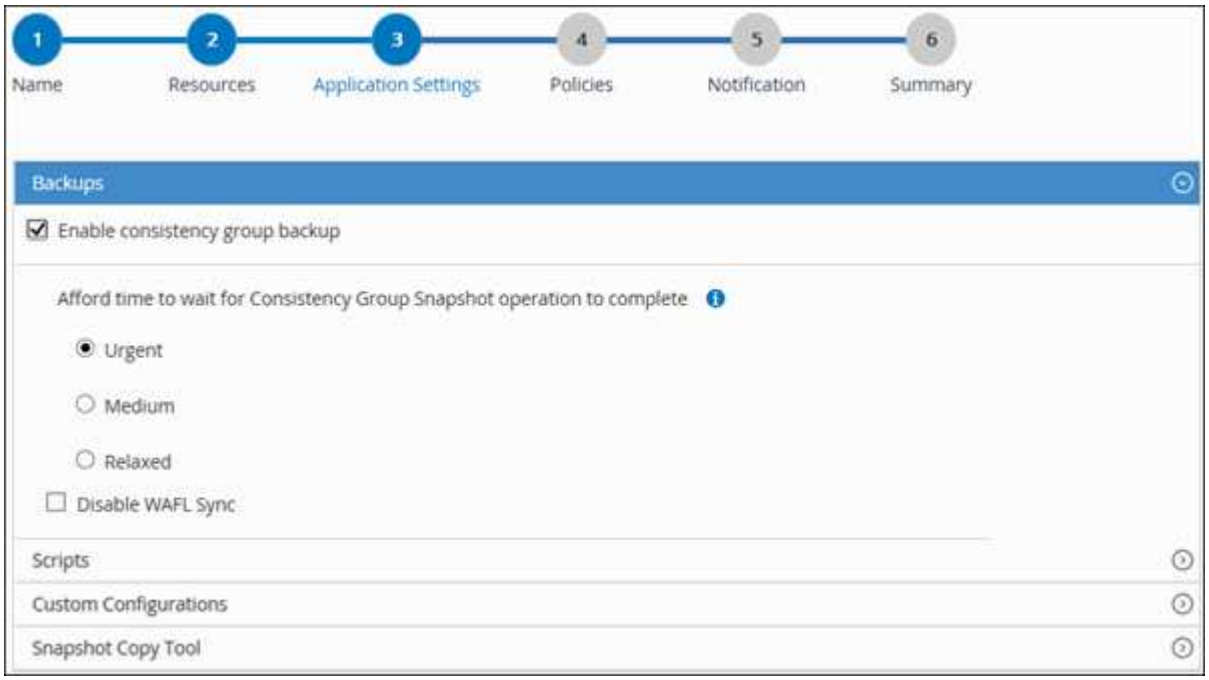
5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus, und wählen Sie dann den Pfeil nach rechts, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Optional: Gehen Sie auf der Seite **Anwendungseinstellungen** wie folgt vor:

   a. Wählen Sie den Pfeil Backups aus, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der Snapshot-Vorgang der Konsistenzgruppe abgeschlossen ist	Wählen Sie dringend, Mittel oder entspannt aus, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+



   a. Wählen Sie den Pfeil für Skripte aus und geben Sie die Befehle vor und nach für Stilllegung, Snapshots und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

   b. Wählen Sie den Pfeil „Benutzerdefinierte Konfigurationen“ aus, und geben Sie die für alle Datenschutzvorgänge, die diese Ressource verwenden, erforderlichen benutzerdefinierten Schlüssel-Wert-Paare ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
ARCHIVE_LOG_DIR	Change_info_Directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

c. Wählen Sie den Pfeil **Snapshot Copy Tool** aus, um das Werkzeug zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu verwenden und das Filesystem vor dem Erstellen eines Snapshots in einen konsistenten Zustand zu versetzen. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus. Diese Option ist für das SnapCenter-Plug-in für SAP HANA Database nicht verfügbar.

Ihre Situation	Dann…
SnapCenter zum Erstellen eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen von Snapshots auf dem Host einzugeben, der ausgeführt werden soll.	Wählen Sie **other** 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 Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie * * auswählen .

      Die Richtlinien sind im Abschnitt * Zeitpläne für ausgewählte Richtlinien konfigurieren* aufgeführt.

   b. Wählen Sie in der Spalte **Configure Schedules** * für die Richtlinie aus , die Sie konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie OK aus.

      Wobei Policy_Name der Name der ausgewählten Richtlinie ist.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt. Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wählen Sie aus der Dropdown-Liste **E-Mail-Präferenz** auf der Seite **Benachrichtigung** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

9. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um Datensicherungsvorgänge durchzuführen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt

werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige Management-LIF-IP-Adresse verfügen.

Schritte

1. Starten Sie eine PowerShell Core-Verbindungssitzung mit dem Cmdlet "Open-SmConnection".

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

   ```
   PS C:\> Open-SmConnection
   ```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Backup einzelner von NetApp unterstützter Plug-ins-Ressourcen

Wenn eine einzelne von NetApp unterstützte Plug-ins-Ressource nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite „Ressourcen“ sichern. Sie können die Ressource nach Bedarf sichern, oder wenn die Ressource über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.

- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Klicken Sie auf , und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann klicken , um den Filterbereich zu schließen.
3. Klicken Sie auf die Ressource, die Sie sichern möchten.
4. Wenn Sie auf der Seite Ressource einen benutzerdefinierten Namen verwenden möchten, aktivieren Sie das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** und geben dann ein benutzerdefiniertes Namensformat für den Snapshot-Namen ein.

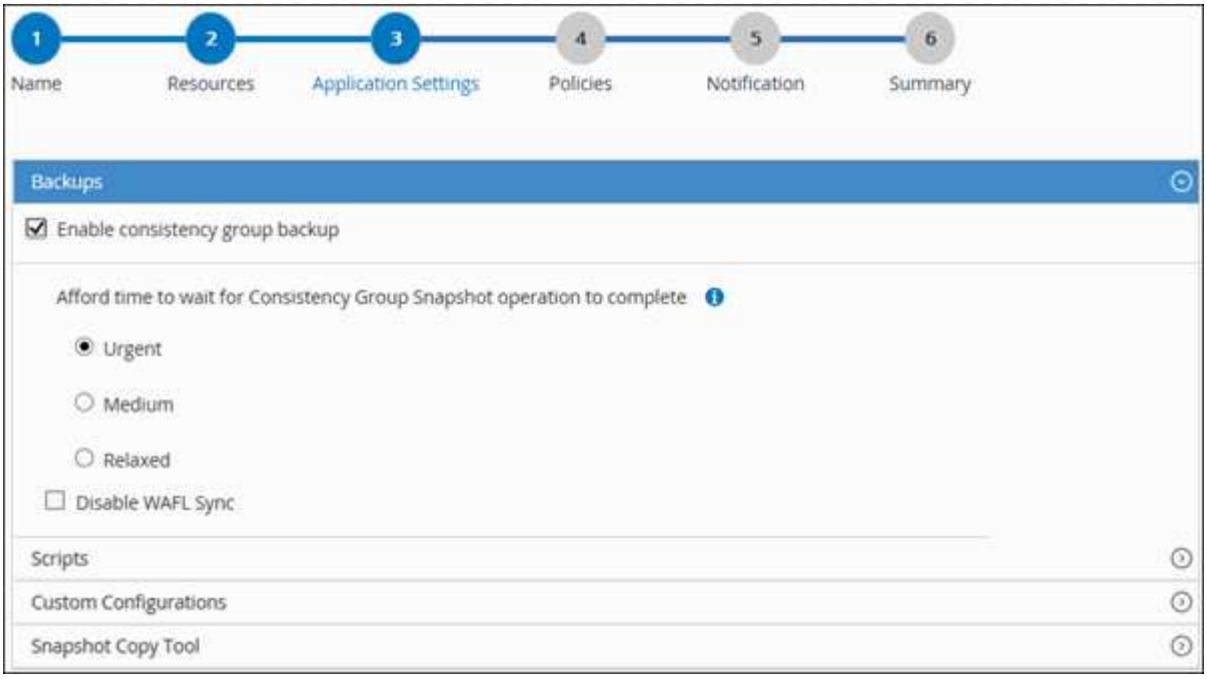
   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.
5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der Snapshot-Vorgang der Konsistenzgruppe abgeschlossen ist	Wählen Sie dringend, Mittel oder entspannt aus, um die Wartezeit für den Snapshot-Vorgang anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   +



a. Klicken Sie auf den Pfeil **Scripts**, um Pre- und Post-Befehle für Stilllegung, Snapshot und Stilllegung auszuführen. Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen.

   Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen**, und geben Sie dann die für alle Aufträge, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.

c. Klicken Sie auf den Pfeil **Snapshot Copy Tool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Ihre Situation	Dann…
SnapCenter zur Erstellung eines Snapshots auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter, um das Filesystem mit dem Plug-in für Windows in einen konsistenten Zustand zu versetzen und anschließend einen Snapshot zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Um den Befehl zum Erstellen eines Snapshots einzugeben	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um einen Snapshot zu erstellen.

6. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

   Sie können eine Richtlinie auch erstellen, indem Sie auf klicken + .

Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf  die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

Dabei ist *Policy_Name* der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Die Seite „Ressourcen-Topologie“ wird angezeigt.

9. Klicken Sie auf **Jetzt sichern**.
10. Führen Sie auf der Seite Backup die folgenden Schritte aus:

a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

b. Klicken Sie Auf **Backup**.

11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-smconnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Mit dem Cmdlet "Add-SmResources" können Sie Ressourcen hinzufügen.

In diesem Beispiel werden Ressourcen hinzugefügt:

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   Dieses Beispiel erstellt eine neue Backup-Richtlinie:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin  -description 'testPolicy'
```

4. Fügen Sie mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter 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.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

   In diesem Beispiel wird ein Job-Summary-Bericht 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.sccore.test.com
```

Backup von Ressourcengruppen von von NetApp unterstützten Plug-in-Ressourcen

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups 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 Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`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 **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf klicken und das Tag auswählen. Sie können dann 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
   - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen. Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei /opt/netapp/init_scvservice. In diesem Skript startet der `do_start method` Befehl den SnapCenter VMware Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Überwachung von Backup-Vorgängen bei von NetApp unterstützten Plug-in-Ressourcen

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung

- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Obwohl der Status des Sicherungsauftrags angezeigt wird , wird beim Klicken auf Jobdetails möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Abbrechen von Backup-Vorgängen für von NetApp unterstützte Plug-ins

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * *  , um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Zeigen Sie auf der Seite „Topologie“ ressourcenbezogene Backups und Klone von NetApp-unterstützten Plug-ins an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen. Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Über diese Aufgabe

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

-  Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.

  Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der

SnapVault-Technologie repliziert werden.

Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie erstellt haben, um nur 4 Backups aufzubewahren, werden die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone angezeigt.

   Durch Klicken auf die Schaltfläche „Aktualisieren“ wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

   Wenn ein SnapLock-fähiges Backup durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die primäre und sekundäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen wird. Ein wöchentlicher Zeitplan aktualisiert auch die primäre und sekundäre SnapLock-Ablaufzeit, die von ONTAP abgerufen wird.

   Wenn die Applikationsressource über mehrere Volumes verteilt ist, ist die SnapLock-Ablaufzeit für das Backup die längste SnapLock-Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock-Ablaufzeit wird von ONTAP abgerufen.

   Nach On-Demand-Backup, durch Klicken auf die Schaltfläche * Aktualisieren* aktualisiert die Details der Sicherung oder des Klons.

5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

   Sie können Backups, die sich auf dem sekundären Speichersystem befinden, nicht umbenennen oder löschen.

Sie können die Backups, die sich auf dem primären Speichersystem befinden, nicht umbenennen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon in der Tabelle aus und klicken Sie auf , um ihn zu löschen.

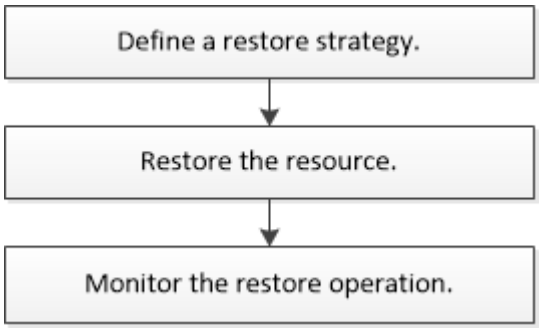
Stellen Sie von NetApp unterstützte Plug-ins-Ressourcen wieder her

Stellen Sie von NetApp unterstützte Plug-in-Ressourcen wieder her

Der Restore- und Recovery-Workflow umfasst Planung, Durchführung von Restore-Vorgängen und Monitoring von Vorgängen.

Über diese Aufgabe

Der folgende Workflow zeigt die Reihenfolge, in der Sie den Wiederherstellungsvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch".

Wiederherstellen eines Ressourcenbackups

Mit SnapCenter können Sie Ressourcen wiederherstellen. Die Funktionen der Restore-Vorgänge hängen vom verwendeten Plug-in ab.

Bevor Sie beginnen

- Sie müssen die Ressource oder Ressourcengruppen gesichert haben.
- Der SnapCenter Administrator muss Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für Ziel-Volumes zugewiesen haben, wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren.
- Sie müssen einen Backup-Vorgang abgebrochen haben, der derzeit für die Ressource oder Ressourcengruppe ausgeführt wird, die wiederhergestellt werden soll.

Über diese Aufgabe

- Der Standardwiederherstellungsvorgang stellt nur Storage-Objekte wieder her. Wiederherstellungen auf Applikationsebene können nur durchgeführt werden, wenn das von NetApp unterstützte Plug-in diese Funktion bietet.
- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den

SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host- oder Cluster-Name, zugeordnete Ressourcengruppen und -Richtlinien sowie der Status angezeigt.

   Obwohl sich ein Backup möglicherweise für eine Ressourcengruppe befindet, müssen Sie bei der Wiederherstellung die einzelnen Ressourcen auswählen, die wiederhergestellt werden sollen.

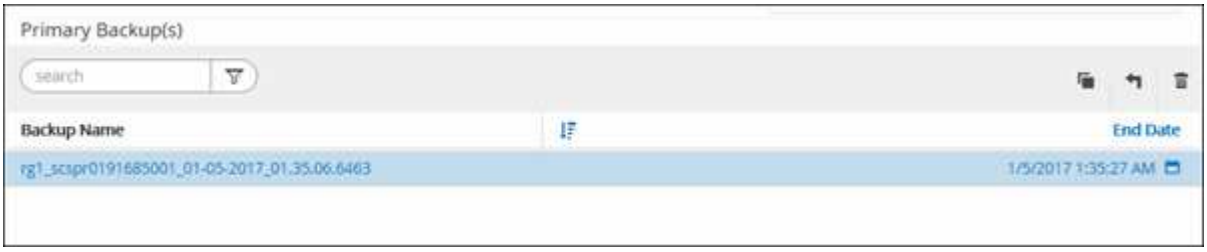
   Wenn die Ressource nicht geschützt ist, wird *Not Protected* in der Spalte **Gesamtstatus** angezeigt.

   Der Status *not protected* 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 aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Kopien verwalten** die Option **Backups** aus den primären oder sekundären (gespiegelten oder gewölbten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, von dem Sie wiederherstellen möchten, und klicken Sie dann auf .



6. Wählen Sie auf der Seite „Bereich wiederherstellen“ die Option **vollständige Ressource** oder **Dateiebene** aus.
   a. Wenn Sie **Complete Resource** ausgewählt haben, wird die Ressourcen-Sicherung wiederhergestellt.

      Wenn die Ressource Volumes oder qtrees als Storage Footprint enthält, werden neuere Snapshots auf diesen Volumes oder qtrees gelöscht und können nicht wiederhergestellt werden. Wenn auch eine andere Ressource auf denselben Volumes oder qtrees gehostet wird, wird diese Ressource ebenfalls gelöscht.

   b. Wenn Sie **File Level** ausgewählt haben, können Sie entweder **Alle** auswählen oder Volumes oder qtrees auswählen und dann den Pfad eingeben, der mit den Volumes oder qtrees verbunden ist, die durch Kommas getrennt ausgewählt werden.

- 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 ausgeführt werden sollen, bevor Sie einen Wiederherstellungsauftrag ausführen.
8. Geben Sie auf der Seite **Post OPS** die Befehle Mount und Post Restore ein, die ausgeführt werden sollen, nachdem ein Wiederherstellungsauftrag ausgeführt wurde.
9. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 an:

```
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 dem Backup mit dem Cmdlet "Restore-SmBackup" wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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          :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Überwachen von Wiederherstellungsvorgängen mit von NetApp unterstützten Plug-in-Ressourcen

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Von NetApp unterstütztes Klon-Plug-in-Ressourcen-Backups

Von NetApp unterstütztes Klon-Plug-in-Ressourcen-Backups

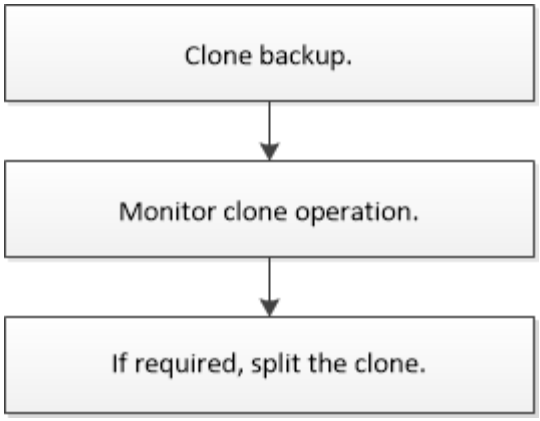
Der Klon-Workflow umfasst die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

Über diese Aufgabe

Sie können Ressourcen-Backups aus den folgenden Gründen klonen:

- Zum Testen von Funktionen, die während der Applikationsentwicklungszyklen mit der aktuellen Ressourcenstruktur und dem aktuellen Inhalt implementiert werden müssen
- Zur Datenextraktion und -Manipulation beim Befüllen von Data Warehouses
- Zum Wiederherstellen von Daten, die versehentlich gelöscht oder geändert wurden

Im folgenden Workflow wird die Sequenz angezeigt, in der Sie den Klonvorgang durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch".

Klonen aus einem Backup

Sie können SnapCenter zum Klonen einer Backup verwenden. Sie können von primärem oder sekundärem Backup klonen. Die Funktionen der Klonvorgänge hängen vom verwendeten Plug-in ab.

Bevor Sie beginnen

- Sie müssen die Ressourcen oder Ressourcengruppe gesichert haben.
- Bei dem Standardklonvorgang werden nur Storage-Objekte geklont. Klonvorgänge auf Applikationsebene können nur durchgeführt werden, wenn das von NetApp unterstützte Plug-in dies ermöglicht.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.

Über diese Aufgabe

Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

UI von SnapCenter

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 **Ansicht** nach Ressourcentyp.

   Die Ressourcen werden zusammen mit Informationen wie Typ, Host- oder Cluster-Name, zugeordnete Ressourcengruppen und -Richtlinien sowie der Status angezeigt.

3. Wählen Sie die Ressource oder Ressourcengruppe aus.

   Sie müssen eine Ressource auswählen, wenn Sie eine Ressourcengruppe auswählen.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Standorte die folgenden Schritte aus:

Für dieses Feld…	Tun Sie das…
Klonserver	Standardmäßig wird der Quell-Host befüllt. Wenn Sie einen anderen Host angeben möchten, wählen Sie den Host aus, auf dem der Klon gemountet werden soll, und das Plug-in ist installiert.
Suffix klonen	Dies ist obligatorisch, wenn das Klonziel mit der Quelle identisch ist. 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. Beispiel: rs1_Clone. Wenn Sie auf demselben Host wie die Originalressource klonen, müssen Sie ein Suffix bereitstellen, um die geklonte Ressource von der ursprünglichen Ressource zu differenzieren. Andernfalls schlägt der Vorgang fehl.

   Wenn die ausgewählte Ressource eine LUN ist und wenn Sie über ein sekundäres Backup klonen, werden die Ziel-Volumes aufgelistet. Es kann mehrere Ziel-Volumes vorhanden sein.

7. Führen Sie auf der Seite **Einstellungen** folgende Schritte aus:

Für dieses Feld…	Tun Sie das…
Name des Initiators	Geben Sie den Host-Initiatornamen ein. Dieser ist entweder ein IQDN oder ein WWPN.
IGroup-Protokoll	Wählen Sie das iGroup-Protokoll aus.

Einstellungsseite wird nur angezeigt, wenn der Speichertyp LUN ist.

8. Geben Sie auf der Seite „Skripts“ die Befehle für den vor- bzw. Nachklon ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

   Beispiel:

   - Befehl Pre Clone: Löschen Sie vorhandene Datenbanken mit demselben Namen
   - Befehl nach Clone: Überprüfen Sie eine Datenbank oder starten Sie eine Datenbank.

     Mount-Befehl für ein Volume oder qtree auf einem Linux-Rechner:
     Mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

9. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben.

10. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

PowerShell Commandlets

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Listen Sie die Backups auf, die mit dem Cmdlet "Get-SmBackup" oder "Get-SmResourceGroup" geklont werden können.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
 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 über eine bestimmte 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                    : {}
    HostResourceMaping          : {}
    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                    : {}
    HostResourceMaping          : {}
    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. Initiieren Sie einen Klonvorgang aus einer Clone Ressourcengruppe oder einer vorhandenen Sicherung mit dem Cmdlet "New-SmClone".

   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 Clone-Jobs mit dem Cmdlet Get-SmCloneReport an.

   In diesem Beispiel wird ein Klonbericht für die angegebene Job-ID angezeigt:

```
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 von NetApp unterstützten Plug-in-Ressourcenklonoperationen

Sie können den Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.

3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
    a. Klicken Sie hier  , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
    b. Geben Sie das Start- und Enddatum an.
    c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
    d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
    e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Schützen Sie Unix-Dateisysteme

Was Sie mit dem SnapCenter-Plug-in für Unix-Dateisysteme tun können

Wenn das Plug-in für Unix-Dateisysteme in Ihrer Umgebung installiert ist, können Sie mit SnapCenter Unix-Dateisysteme sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Und entdecken Sie Ressourcen
- Sichern Sie Unix-Dateisysteme
- Planen von Backup-Vorgängen
- Wiederherstellung von Dateisystemsicherungen
- Backups von Dateisystemen klonen
- Monitoring von Backup-, Restore- und Klonvorgängen

Unterstützte Konfigurationen

Element	Unterstützte Konfiguration
Umgebungen Beschrieben Sind	• Physischer Server • Virtueller Server VVol Datastores auf NFS und SAN. VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
File-Systeme	• SAN ◦ Sowohl LVM- als auch nicht-LVM-basierte Dateisysteme ◦ LVM über VMDK ext3, ext4 und xfs • NFS: NFS v3, NFS v4.x
Protokolle	• FC • FCoE • ISCSI • NFS

Element	Unterstützte Konfiguration
Multipath	ja

Einschränkungen

- Die Kombination aus RDMs und virtuellen Laufwerken in einer Volume-Gruppe wird nicht unterstützt.
- Wiederherstellung auf Dateiebene wird nicht unterstützt.

  Sie können jedoch manuell Wiederherstellungen auf Dateiebene durchführen, indem Sie das Backup klonen und die Dateien dann manuell kopieren.

- Kombination aus auf VMDKs verteilten Filesystemen, die sowohl von NFS- als auch von VMFS-Datastore stammen, wird nicht unterstützt.
- NVMe wird nicht unterstützt.
- Bereitstellung wird nicht unterstützt.

Installieren Sie das SnapCenter-Plug-in für Unix-Dateisysteme

Voraussetzungen für das Hinzufügen von Hosts und das Installieren von Plug-ins Package für Linux

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.

  Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.

- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

  > Stellen Sie sicher, dass Sie nur die zertifizierte Version VON JAVA 11 auf dem Linux-Host installiert haben.

  Informationen zum Herunterladen von JAVA finden Sie unter: "Java-Downloads für alle Betriebssysteme"

- Sie sollten **bash** als Standard-Shell für die Plug-in-Installation haben.

Linux Host-Anforderungen

Bevor Sie das SnapCenter-Plug-ins-Paket für Linux installieren, sollten Sie sicherstellen, dass der Host die Anforderungen erfüllt.

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
MindestRAM für das SnapCenter Plug-in auf dem Host	2GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Stellen Sie sicher, dass Sie nur die zertifizierte Version VON JAVA 11 auf dem Linux-Host installiert haben. Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Fügen Sie Hosts hinzu und installieren Sie Plug-ins Package for Linux mithilfe der GUI

Sie können die Seite Host hinzufügen verwenden, um Hosts hinzuzufügen und anschließend das SnapCenter-Plug-ins-Paket für Linux zu installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:

Für dieses Feld…	**Tun Sie das…**
Host-Typ	Wählen Sie **Linux** als Hosttyp aus.
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt zu installierende Plug-ins auswählen **Unix-Dateisysteme** aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer ist 8145. Wenn der SnapCenter-Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist */opt/NetApp/snapcenter*. Optional können Sie den Pfad anpassen. Wenn Sie den benutzerdefinierten Pfad verwenden, stellen Sie sicher, dass der Standardinhalt der Sudoers mit dem benutzerdefinierten Pfad aktualisiert wird.
Überspringen Sie optionale Prüfungen vor der Installation	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen Vorabprüfungen nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

   Das Precheck-Skript überprüft den Firewall-Status des Plug-in-Ports nicht, wenn er in den Regeln für die Ablehnung der Firewall angegeben ist.

   Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt. Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter *C:\Program Files\NetApp\SnapCenter WebApp* aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, sollten Sie das Problem beheben.

   Wenn Sie in einem HA-Setup die Datei „Web.config“ aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

8. Überprüfen Sie den Fingerabdruck, und klicken Sie dann auf **Bestätigen und Senden**.

   SnapCenter unterstützt keinen ECDSA-Algorithmus.

Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Log-Dateien befinden sich unter */Custom_Location/snapcenter/logs*.

Ergebnis

Alle auf dem Host gemounteten Dateisysteme werden automatisch erkannt und auf der Seite „Ressourcen“ angezeigt. Wenn nichts angezeigt wird, klicken Sie auf **Ressourcen aktualisieren**.

Überwachung des Installationsstatus

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet werden, gehen Sie wie folgt vor:
   a. Klicken Sie Auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü Typ die Option **Plug-in Installation**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst

Der SnapCenter-Plug-in-Loader-Dienst lädt das Plug-in-Paket, damit Linux mit dem SnapCenter-Server interagieren kann. Der SnapCenter-Plug-in-Loader-Dienst wird installiert, wenn Sie das SnapCenter-Plug-ins-Paket für Linux installieren.

Über diese Aufgabe

Nach der Installation des SnapCenter-Plug-ins-Pakets für Linux wird der SnapCenter-Plug-in-Loader-Dienst automatisch gestartet. Wenn der SnapCenter-Plug-in-Loader-Dienst nicht automatisch gestartet wird, sollten Sie Folgendes tun:

- Stellen Sie sicher, dass das Verzeichnis, in dem das Plug-in ausgeführt wird, nicht gelöscht wird
- Erhöhen Sie den Speicherplatz, der der Java Virtual Machine zugewiesen ist

Die Datei spl.properties befindet sich unter */Custom_Location/NetApp/snapcenter/spl/etc/* und enthält die folgenden Parameter: Diesen Parametern werden Standardwerte zugewiesen.

Parametername	Beschreibung
PROTOKOLL_LEVEL	Zeigt die unterstützten Protokollebenen an. Mögliche Werte sind TRACE, DEBUG, INFO, WARN, FEHLER, Und TÖDLICH.
SPL_PROTOKOLL	Zeigt das von SnapCenter Plug-in Loader unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SNAPCENTER_SERVER_PROTOCOL	Zeigt das von SnapCenter-Server unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SKIP_JAVAHOME_UPDATE	Standardmäßig erkennt der SPL-Dienst den java-Pfad und aktualisiert DEN JAVA_HOME-Parameter. Daher ist der Standardwert AUF FALSE gesetzt. Sie können auf „TRUE“ setzen, wenn Sie das Standardverhalten deaktivieren und den java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Kennwort der Schlüsselspeicherdatei an. Sie können diesen Wert nur ändern, wenn Sie das Passwort ändern oder eine neue Schlüsselspeicherdatei erstellen.

Parametername	Beschreibung
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Plug-in-Loader ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt. Nach der Installation der Plug-ins sollten Sie den Wert nicht ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter-Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Schlüsselspeicherdatei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.
„LOGS_MAX_COUNT“	Zeigt die Anzahl der SnapCenter-Plug-in-Loader-Protokolldateien an, die im Ordner */Custom_location/snapcenter/spl/logs* aufbewahrt werden. Der Standardwert ist 5000. Wenn der Zähler größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Prüfung auf die Anzahl der Dateien erfolgt automatisch alle 24 Stunden ab dem Start des SnapCenter Plug-in Loader-Dienstes. Wenn Sie die Datei spl.properties manuell löschen, wird die Anzahl der zu behaltenden Dateien auf 9999 festgelegt.
JAVA_HOME	Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird. Dieser Pfad wird während der Installation und im Rahmen des Startens von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Log-Datei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei gezippt und die Protokolle werden in die neue Datei dieses Jobs geschrieben.

Parametername	Beschreibung
BEIBEHALTEN_LOGS_OF_LAST_DAYS	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
ENABLE_CERTIFICATE_VALIDATION	Zeigt true an, wenn die Zertifikatvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder aktivieren oder deaktivieren, indem Sie den spl.properties bearbeiten oder den SnapCenter GUI oder Cmdlet verwenden.

Wenn einer dieser Parameter dem Standardwert nicht zugewiesen ist oder Sie den Wert zuweisen oder ändern möchten, können Sie die Datei spl.properties ändern. Sie können auch die Datei spl.properties überprüfen und die Datei bearbeiten, um Probleme zu beheben, die mit den Werten, die den Parametern zugeordnet sind, zusammenhängen. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter-Plug-in-Loader-Dienst neu starten.

Schritte

1. Führen Sie bei Bedarf eine der folgenden Aktionen aus:
   - Starten Sie den SnapCenter-Plug-in-Loader-Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Stoppen Sie den SnapCenter-Plug-in-Loader-Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     Sie können die Option -Force mit dem Befehl STOP verwenden, um den SnapCenter Plug-in Loader Dienst nachdrücklich zu stoppen. Vor diesem Verfahren sollten Sie jedoch Vorsicht walten lassen, da auch die bestehenden Vorgänge beendet werden.
   - Starten Sie den SnapCenter-Plug-in-Loader-Dienst neu:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Suchen Sie den Status des SnapCenter-Plug-in-Loader-Dienstes:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl status`

- Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Finden Sie die Änderung im SnapCenter-Plug-in-Loader-Dienst:

- Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Führen Sie als Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Service auf dem Linux-Host

Sie sollten das Passwort von SPL Keystore und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für SPL Trust-Store konfigurieren und das CA-signierte Schlüsselpaar für SPL Trust-Store mit dem SnapCenter Plug-in Loader Service konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

SPL verwendet die Datei 'keystore.jks', die sich bei '/var/opt/snapcenter/spl/etc' sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für SPL-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen.

   Dieser Wert entspricht dem Schlüssel 'SPL_KEYSTORE_PASS'.

2. Ändern Sie das Schlüsselspeicher-Passwort:

```
 keytool -storepasswd -keystore keystore.jks
. Ändern Sie das Kennwort für alle Aliase privater Schlüsseleinträge im Schlüsselspeicher auf dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Aktualisieren Sie das gleiche für den Schlüssel SPL_KEYSTORE_PASS in der Datei spl.properties.

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

Passwort für SPL-Schlüsselspeicher und für alle zugeordneten Alias-Passwort des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel in den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher: */var/opt/snapcenter/spl/etc*.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie ein Stammzertifikat oder ein Zwischenzertifikat hinzu:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stammzertifikate oder
Zwischenzertifikate in den SPL Trust-Store konfiguriert haben.
```

Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar für SPL Trust-Store

Sie sollten das CA-signierte Schlüsselpaar für den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Schlüsselspeicher /var/opt/snapcenter/spl/etc. Enthält
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen
Schlüssel hinzu.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.
```

```
 keytool -list -v -keystore keystore.jks
. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält,
der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher
hinzugefügt wurde.
. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für
das CA-Zertifikat in das Schlüsselspeicher-Passwort.
```

Das Standard-SPL-Schlüsselspeicherkennwort ist der Wert des Schlüssels SPL_KEYSTORE_PASS in der Datei spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Wenn der Alias-Name im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen enthält („*","","), ändern Sie den Alias-Namen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Konfigurieren Sie den Alias-Namen aus dem Schlüsselspeicher, der sich
in der Datei spl.properties befindet.
```

Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.

4. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

- SPL wird nach den CRL-Dateien in einem vorkonfigurierten Verzeichnis suchen.
- Das Standardverzeichnis für die CRL-Dateien für SPL lautet */var/opt/snapcenter/spl/etc/crl*.

Schritte

1. Sie können das Standardverzeichnis in der Datei spl.properties mit dem Schlüssel SPL_CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss angezeigt, und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- Gibt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-in-Host zugewiesen ist.
- Zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- Zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- Zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

> Wenn der Status gelb oder grün lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

Wenn Ihre Datenbank oder Ihr Dateisystem auf virtuellen Maschinen (VMs) gespeichert ist oder Sie VMs und Datastores schützen möchten, müssen Sie das virtuelle SnapCenter-Plug-in für VMware vSphere-Gerät bereitstellen.

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

Informationen zum Konfigurieren des CA-Zertifikats mit SnapCenter-Plug-in für VMware vSphere finden Sie unter "Erstellen oder importieren Sie ein SSL-Zertifikat".

Konfigurieren Sie die CRL-Datei

Das SnapCenter Plug-in für VMware vSphere sucht die CRL-Dateien in einem vorkonfigurierten Verzeichnis. Das Standardverzeichnis der CRL-Dateien für das SnapCenter Plug-in für VMware vSphere ist */opt/netapp/config/crl*.

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Bereiten Sie sich auf den Schutz von Unix-Dateisystemen vor

Bevor Sie Datensicherungsvorgänge wie z. B. Backup-, Klon- oder Restore-Vorgänge durchführen, sollten Sie Ihre Umgebung einrichten. Sie können den SnapCenter Server auch zur Verwendung von SnapMirror und SnapVault Technologie einrichten.

Um von der SnapVault und SnapMirror Technologie zu profitieren, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes auf dem Storage-Gerät konfigurieren und initialisieren. Sie können entweder NetApp System Manager verwenden oder die Storage-Konsole verwenden, um diese Aufgaben auszuführen.

Bevor Sie das Plug-in für Unix-Dateisysteme verwenden, muss der SnapCenter-Administrator den SnapCenter-Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installation und Konfiguration des SnapCenter-Servers "Weitere Informationen ."
- Konfigurieren Sie die SnapCenter-Umgebung durch Hinzufügen von Storage-Systemverbindungen. "Weitere Informationen ."

> SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede für SnapCenter registrierte SVM, die eine SVM-Registrierung oder eine Cluster-Registrierung verwendet, muss eindeutig sein.

- Fügen Sie Hosts hinzu, installieren Sie die Plug-ins und ermitteln Sie die Ressourcen.
- Wenn Sie SnapCenter-Server zum Schutz von Unix-Dateisystemen verwenden, die sich auf VMware RDM-LUNs oder VMDKs befinden, müssen Sie das SnapCenter-Plug-in für VMware vSphere implementieren und das Plug-in bei SnapCenter registrieren.
- Installieren Sie Java auf Ihrem Linux-Host.
- Konfigurieren Sie SnapMirror und SnapVault auf ONTAP, wenn Sie Backup-Replizierung möchten.

Sichern Sie Unix-Dateisysteme

Ermitteln Sie die für Backups verfügbaren UNIX-Dateisysteme

Nach der Installation des Plug-ins werden alle Dateisysteme auf diesem Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt. Sie können diese Dateisysteme zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge auszuführen.

Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Wenn sich die Dateisysteme auf einem virtuellen Maschinenlaufwerk (VMDK) oder Raw Device Mapping (RDM) befinden, müssen Sie das SnapCenter-Plug-in für VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Implementieren Sie das SnapCenter Plug-in für VMware vSphere".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste Ansicht die Option **Pfad** aus.
3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   Die Dateisysteme werden zusammen mit Informationen wie Typ, Hostname, zugeordnete Ressourcengruppen und Richtlinien sowie Status angezeigt.

Erstellen Sie Backup-Richtlinien für Unix-Dateisysteme

Bevor Sie SnapCenter zum Sichern von Unix-Dateisystemen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln. Sie können auch die Einstellungen für Replikation, Skript und Backup-Typ festlegen. Das Erstellen einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressource oder Ressourcengruppe wiederverwenden möchten.

Bevor Sie beginnen

- Sie müssen sich auf die Datensicherung vorbereitet haben, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erkennen der Dateisysteme und das Erstellen von Storage-System-Verbindungen durchführen.
- Wenn Sie Snapshots auf einen sekundären gespiegelten oder Vault-Storage replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Ziel-Volumes zugewiesen haben.
- Prüfen Sie die spezifischen Voraussetzungen und Einschränkungen von SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektgrenzen für die aktive SnapMirror Synchronisierung".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Wählen Sie **Unix File Systems** aus der Dropdown-Liste aus.
4. Klicken Sie Auf **Neu**.
5. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
6. Geben Sie die Zeitplanhäufigkeit an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.
7. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den

auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Total Snapshot Copies to keep** aus, und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Snapshot-Kopien behalten für**, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots vor dem Löschen behalten möchten.

Sie können Archiv-Protokoll-Backups nur dann aufbewahren, wenn Sie die Archiv-Log-Dateien als Teil Ihrer Sicherung ausgewählt haben.

8. Geben Sie auf der Seite Replikation die Replikationseinstellungen an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Diese Option sollte für SnapMirror Active Sync aktiviert sein.
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen.
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um die maximale Grenze von Snapshots auf dem sekundären Storage zu vermeiden.

9. Geben Sie auf der Seite Skript den Pfad und die Argumente des Prescript oder Postscript ein, das Sie vor oder nach dem Backup ausführen möchten.

   Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host verfügbar ist, über den Pfad _ /opt/NetApp/SnapCenter/scc/etc/allowed_commands.config_.

   Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Unix-Dateisysteme

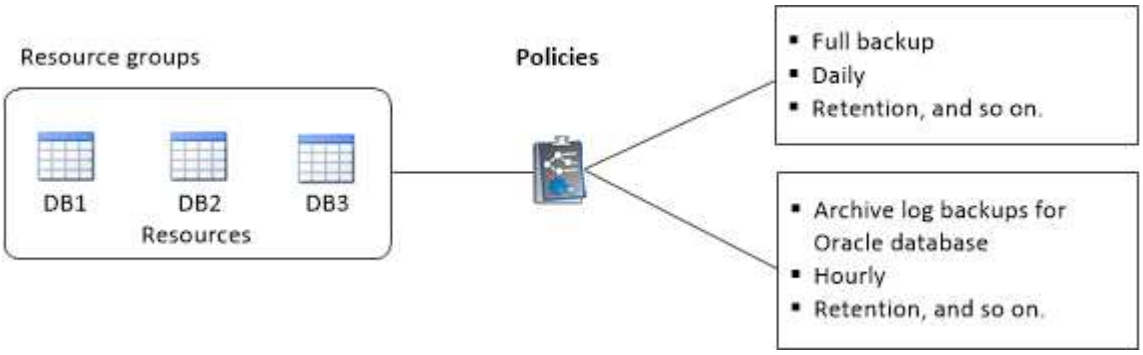
Eine Ressourcengruppe ist ein Container, in dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten sichern, die mit den Dateisystemen verknüpft sind.

Über diese Aufgabe

- Eine Datenbank mit Dateien in ASM-Datenträgergruppen muss sich im „MOUNT“- oder „OPEN“-Zustand befinden, um ihre Backups mit dem Dienstprogramm Oracle DBVERIFY zu überprüfen.

  Fügen Sie der Ressourcengruppe eine oder mehrere Richtlinien hinzu, um den Typ des Datenschutzauftrags zu definieren, den Sie ausführen möchten.

  Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



- Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Das Hinzufügen neuer Dateisysteme ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Dateisysteme zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Status Ressourcen hinzufügen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf der Seite Ressourcen auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   a. Geben Sie im Feld Name einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

   b. Geben Sie eine oder mehrere Beschriftungen in das Feld Tag ein, um später nach der Ressourcengruppe zu suchen.

      Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.

c. Aktivieren Sie das Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

   Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Host-Namen für Unix-Dateisysteme aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden im Abschnitt Verfügbare Ressourcen nur dann aufgelistet, wenn die Ressource erfolgreich ermittelt wurde. Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

5. Wählen Sie im Abschnitt Verfügbare Ressourcen die Ressourcen aus, und verschieben Sie sie in den Abschnitt Ausgewählte Ressourcen.
6. Führen Sie auf der Seite Anwendungseinstellungen die folgenden Schritte aus:
   - Wählen Sie den Pfeil für Skripte aus und geben Sie die Befehle vor und nach für Stilllegung, Snapshots und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.
   - Wählen Sie eine der Backup-Konsistenzoptionen aus:
     - Wählen Sie **File System consistent** aus, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden und keine ein- oder Ausgabevorgänge im Dateisystem während der Erstellung der Sicherung erlaubt sind.

       Für File-System-konsistente Snapshots werden für LUNs, die in der Volume-Gruppe beteiligt sind, Snapshots von Konsistenzgruppen erstellt.

     - Wählen Sie **Crash-konsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden.

       Wenn Sie verschiedene Dateisysteme in der Ressourcengruppe hinzugefügt haben, werden alle Volumes aus verschiedenen Dateisystemen in der Ressourcengruppe in eine Konsistenzgruppe aufgenommen.

7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf klicken  .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf  die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Fenster Add Schedules for Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

Dabei ist *Policy_Name* der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Sichern Sie Unix-Dateisysteme

Wenn eine Ressource nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste Ansicht die Option **Pfad** aus.
3. Klicken Sie auf , und wählen Sie dann den Hostnamen und die Unix-Dateisysteme aus, um die Ressourcen zu filtern.
4. Wählen Sie das Dateisystem aus, das Sie sichern möchten.
5. Auf der Seite „Ressourcen“ können Sie die folgenden Schritte ausführen:
   a. Aktivieren Sie das Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

      Zum Beispiel, `customtext_policy_hostname` oder `resource_hostname`. Standardmäßig wird ein Zeitstempel an den Snapshot Namen angehängt.

6. Führen Sie auf der Seite Anwendungseinstellungen die folgenden Schritte aus:
   - Wählen Sie den Pfeil für Skripte aus und geben Sie die Befehle vor und nach für Stilllegung, Snapshots und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.
   - Wählen Sie eine der Backup-Konsistenzoptionen aus:
     - Wählen Sie **File System consistent** aus, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden und keine Vorgänge auf dem Dateisystem während der Erstellung der Sicherung ausgeführt werden.
     - Wählen Sie **Crash-konsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden.

7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie erstellen, indem Sie auf klicken .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf , um einen Zeitplan für die gewünschte Richtlinie zu konfigurieren.

   c. Konfigurieren Sie im Fenster Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann `OK`.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen die E-Mail-Adressen von Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des auf der Ressource durchgeführten Sicherungsvorgangs anhängen möchten, wählen Sie **Job-Bericht anhängen**.

   Für E-Mail-Benachrichtigungen müssen Sie die SMTP-Serverdetails entweder über die GUI oder über den PowerShell-Befehl angegeben haben `Set-SmSmtpServer`.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Topologieseite wird angezeigt.

10. Klicken Sie auf **Jetzt sichern**.
11. Führen Sie auf der Seite Backup die folgenden Schritte aus:

    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste Richtlinie die Richtlinie aus, die Sie für das Backup verwenden möchten.

       Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

    b. Klicken Sie Auf **Backup**.

12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Erstellen Sie ein Backup von Ressourcengruppen für Unix-Dateisysteme

Sie können die in der Ressourcengruppe definierten Unix-Dateisysteme sichern. Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn einer Ressourcengruppe eine Richtlinie angehängt und ein Zeitplan

konfiguriert ist, werden Backups gemäß dem Zeitplan erstellt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.
3. Geben Sie den Namen der Ressourcengruppe in das Suchfeld ein, oder klicken Sie auf , und wählen Sie das Tag aus.

   Klicken Sie auf , um das Filterfenster zu schließen.
4. Wählen Sie auf der Seite Ressourcengruppe die Ressourcengruppe aus, die gesichert werden soll.
5. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie mehrere Richtlinien mit der Ressourcengruppe verknüpft haben, wählen Sie die zu verwendende Sicherungsrichtlinie aus der Dropdown-Liste **Policy** aus.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Wählen Sie **Backup**.
6. Überwachen Sie den Fortschritt, indem Sie **Monitor > Jobs** auswählen.

Überwachen Sie das Backup von Unix-Dateisystemen

Erfahren Sie, wie Sie den Fortschritt von Backup-Vorgängen und Datensicherungsvorgängen überwachen.

Überwachen Sie die Backup-Vorgänge für Unix-Dateisysteme

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.

3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Obwohl der Status des Sicherungsauftrags angezeigt wird , wird beim Klicken auf Jobdetails möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen Sie Datensicherungsvorgänge im Teilfenster „Vorgang“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Job-Details** aufgeführt.

Zeigen Sie geschützte Unix-Dateisysteme auf der Seite Topologie an

Wenn Sie die Erstellung von Backups, Wiederherstellungen oder Klonvorgängen für eine Ressource vorbereiten, ist es möglicherweise hilfreich, eine grafische Darstellung aller Backups, wiederhergestellten Dateisysteme und Klone im primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

Auf der Seite Topologie werden alle Backups, wiederhergestellten Dateisysteme und Klone angezeigt, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details zu diesen Backups, wiederhergestellten Dateisystemen und Klonen anzeigen und sie dann auswählen, um Datensicherungsvorgänge durchzuführen.

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

-  Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.

  Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Wenn Sie eine sekundäre Beziehung als SnapMirror Active Sync haben (ursprünglich als SnapMirror Business Continuity [SM-BC] veröffentlicht), werden die folgenden zusätzlichen Symbole angezeigt:

-  Der Replikatstandort ist hochgefahren.
-  Der Replikatstandort ist ausgefallen.
-  Die sekundäre Spiegel- oder Vault-Beziehung wurde nicht wiederhergestellt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone angezeigt.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

   Wenn ein SnapLock-fähiges Backup durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die primäre und sekundäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen

wird. Ein wöchentlicher Zeitplan aktualisiert auch die primäre und sekundäre SnapLock-Ablaufzeit, die von ONTAP abgerufen wird.

Wenn das Dateisystem über mehrere Volumes verteilt ist, ist die SnapLock-Ablaufzeit für das Backup die längste SnapLock-Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock-Ablaufzeit wird von ONTAP abgerufen.

Bei aktiver SnapMirror-Synchronisierung wird durch Klicken auf die Schaltfläche * Aktualisieren* das SnapCenter-Backup-Inventar aktualisiert, indem ONTAP sowohl für primäre als auch für Replikatstandorte abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken durch, die die aktive SnapMirror Synchronisierung enthalten.

- Bei aktiver SnapMirror Synchronisierung und nur für ONTAP 9.14.1 sollten die Beziehungen zwischen Async Mirror und Async MirrorVault zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault automatisch auf das neue primäre Ziel konfiguriert.
- Nach dem Failover sollte ein Backup erstellt werden, damit SnapCenter den Failover erkennt. Sie können erst dann auf **Refresh** klicken, wenn ein Backup erstellt wurde.

5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf die Datensicherungssymbole, um Restore-, Klon- und Löschvorgänge durchzuführen.

   Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .

Beispiel für Backups und Klone auf dem Primärspeicher

Stellen Sie Unix-Dateisysteme wieder her

Stellen Sie Unix-Dateisysteme wieder her

Im Falle eines Datenverlustes können Sie SnapCenter verwenden, um Unix-Dateisysteme wiederherzustellen.

Über diese Aufgabe

- Sie sollten die folgenden Befehle ausführen, um die Verbindung zum SnapCenter-Server herzustellen, die Backups aufzulisten, seine Informationen abzurufen und die Sicherung wiederherzustellen.

  Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von get-Help *Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Command Reference Guide".

- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup vom primären Speicherort auswählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder **Pfad** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.

3. Wählen Sie das Dateisystem entweder in der Detailansicht oder in der Detailansicht der Ressourcengruppe aus.

   Die Topologieseite wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Gehen Sie auf der Seite Wiederherstellungsumfang wie folgt vor:
   - Bei NFS-Dateisystemen ist standardmäßig **Connect and Copy** Restore ausgewählt. Sie können auch **Volume Revert** oder **Fast Restore** auswählen.
   - Für Dateisysteme, die kein NFS sind, wird der Wiederherstellungsumfang abhängig vom Layout ausgewählt.

     Die neuen Dateien, die nach der Sicherung erstellt wurden, sind nach der Wiederherstellung möglicherweise nicht verfügbar, je nach Typ und Layout des Dateisystems.
7. Geben Sie auf der Seite PreOps die vor der Wiederherstellung ausgeführten Befehle ein, bevor Sie einen Wiederherstellungsjob ausführen.
8. Geben Sie auf der PostOps-Seite Post-Restore-Befehle ein, die nach der Durchführung eines Wiederherstellungsjobs ausgeführt werden sollen.

   Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host unter der Adresse */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config* Pfad verfügbar ist.

9. Wählen Sie auf der Seite Benachrichtigung aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den ausgeführten Wiederherstellungsvorgang anhängen möchten, müssen Sie **Job-Bericht anhängen** auswählen.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

    Wenn der Wiederherstellungsvorgang fehlschlägt, wird ein Rollback nicht unterstützt.

    Bei der Wiederherstellung eines Dateisystems, das sich auf der Volume-Gruppe befindet, werden die alten Inhalte im Dateisystem nicht gelöscht. Nur der Inhalt des geklonten Dateisystems wird in das Quelldateisystem kopiert. Dies gilt, wenn mehrere Dateisysteme auf der Volume-Gruppe und standardmäßige NFS-Dateisystemwiederherstellungen vorhanden sind.

11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Überwachen Sie die Wiederherstellungsvorgänge von Unix-Dateisystemen

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Klonen von Unix-Dateisystemen

Klonen des Unix Filesystem-Backups

Sie können SnapCenter verwenden, um Unix-Dateisystem mit dem Backup des Dateisystems zu klonen.

Bevor Sie beginnen

- Sie können die Aktualisierung der fstab-Datei überspringen, indem Sie den Wert von *SKIP_FSTAB_UPDATE* auf **true** in der Datei *agent.properties* unter */opt/NetApp/snapcenter/scc/etc* setzen.
- Sie können einen statischen Klon-Volume-Namen und einen Verbindungspfad erhalten, indem Sie den Wert von *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* in der Datei *agent.properties* unter */opt/NetApp/snapcenter/scc/etc* auf **true** setzen. Nach der Aktualisierung der Datei sollten Sie den SnapCenter Plug-in Creator-Dienst neu starten, indem Sie den folgenden Befehl ausführen: `/opt/NetApp/snapcenter/scc/bin/scc restart`.

  Beispiel: Ohne diese Eigenschaft werden der Name des geklonten Volumes und der Verbindungspfad wie <Source_volume_name>_Clone_<Timestamp> sein, aber jetzt wird es <Source_volume_name>_Clone_<Clone_Name> sein

  Dadurch bleibt der Name konstant, so dass Sie die fstab-Datei manuell aktualisieren können, wenn Sie es nicht vorziehen, den fstab von SnapCenter zu aktualisieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder **Pfad** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie das Dateisystem entweder in der Detailansicht oder in der Detailansicht der Ressourcengruppe aus.

   Die Topologieseite wird angezeigt.
4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (sekundär) aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Standardmäßig wird der Quell-Host befüllt.
Mount-Punkt klonen	Geben Sie den Pfad an, auf den das Dateisystem gemountet werden soll.

7. Führen Sie auf der Seite Skripts die folgenden Schritte aus:
   a. Geben Sie die Befehle für den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.

      Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host verfügbar ist, und zwar über den Pfad */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail

angeben. Wenn Sie den Bericht über den ausgeführten Klonvorgang anhängen möchten, wählen Sie **Job-Bericht anhängen** aus.

> Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Teilen Sie einen Klon auf

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon ist unabhängig von der übergeordneten Ressource.

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Einschränkungen des Vorgangs für die Klonaufteilung finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System online ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite **Ressourcen** die entsprechende Option aus der Liste Ansicht aus:

Option	Beschreibung
Für Datenbankapplikationen	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Für File-Systeme	Wählen Sie in der Liste Ansicht **Pfad** aus.

3. Wählen Sie die entsprechende Ressource aus der Liste aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Manage Copies** die geklonte Ressource aus (z. B. die Datenbank oder LUN), und klicken Sie dann auf *  .

5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Clone-Splitvorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet "Stop-SmJob" ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragzeit benötigen, um zu prüfen, ob der Klon geteilt ist oder nicht, können Sie den Wert von *CloneSplitStatusCheckPollTime* Parameter in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Clone Split-Vorgangs angezeigt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klontrennung schlägt fehl, wenn gerade Backup-, Wiederherstellungs- oder andere Klonsplitonen durchgeführt werden. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Verwandte Informationen

"Der SnapCenter Klon oder die Überprüfung schlägt fehl, wenn das Aggregat nicht vorhanden ist"

Überwachen Sie die Klonvorgänge von Unix-Dateisystemen

Sie können den Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:

a. Klicken Sie hier  , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
b. Geben Sie das Start- und Enddatum an.
c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.

4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Sichern Sie Applikationen, die auf Azure NetApp Files ausgeführt werden

Sichern Sie Applikationen, die auf Azure NetApp Files ausgeführt werden

SnapCenter unterstützt den Schutz von Applikationen wie Oracle, SQL und SAP HANA, die auf Azure NetApp Files residieren. Ab Version 6.0.1 unterstützt SnapCenter die Backup-Funktion Azure NetApp Files, die die Datensicherungsfunktionen von Azure NetApp Files durch eine vollständig gemanagte Backup-Lösung für langfristiges Recovery, Archivierung und Compliance erweitert.

Azure NetApp Files ist eine Storage-Lösung der Premiumklasse für die langfristige Backup-Aufbewahrung und kann teuer sein. Zur Kostenoptimierung können Sie die Backups aus dem Azure NetApp Files Storage in einen Azure Objektspeicher verschieben. Ab SnapCenter 6.0 können Sie Backups von Applikationen auf Azure NetApp Files in Azure Blob Storage (Objektspeicher) erstellen und klonen. Sie können zwei Kopien Ihrer Daten aufbewahren, Volume-Snapshot-Kopien auf Azure NetApp Files Storage für die kurzfristige Recovery und eine weitere Kopie auf Azure Blob Storage für die langfristige Recovery.

Wenn eine Richtlinie mit Azure NetApp Files Backup aktiviert ist und einer Ressource zugeordnet ist, übernimmt SnapCenter die Erstellung von Volume-Snapshots und das Backup auf Azure Blob Storage. SnapCenter erstellt den Backup-Vault und ermöglicht die Sicherung für das Volume. Wenn Sie das Backup für das Volume aktiviert haben, verwendet SnapCenter das vorhandene Vault.

Einschränkungen

- Objekt-Storage-Funktionen für FAS oder AFF ONTAP und FSxN Storage-Systeme werden nicht unterstützt.
- Mount- und Katalog-Workflows für Oracle und SAP HANA werden für Objekt-Storage-Backups nicht unterstützt, sondern für Snapshots unterstützt.
- Oracle PDB-Klone werden für Objektspeicher-Backups nicht unterstützt, aber für Snapshots werden unterstützt.
- Backup-Überprüfung auf Basis von Objekt-Storage, Unterstützung für REST-API, Lifecycle Management für Klone aus Objekt-Storage und Berichterstellungsfunktionen für Objekt-Storage-Backups werden nicht unterstützt.
- Die Wiederherstellung aus Backups auf Azure Blob Storage in Azure NetApp Files wird nicht unterstützt. Sie können alternativ die Option Klonen verwenden.
- Die Klonaufteilung wird nicht unterstützt.

Installieren Sie SnapCenter und erstellen Sie Anmeldeinformationen

Installieren Sie SnapCenter auf der Azure Virtual Machine

Sie können die SnapCenter-Software von der NetApp-Support-Website herunterladen und die Software auf der virtuellen Azure-Maschine installieren.

Bevor Sie beginnen

- Vergewissern Sie sich, dass die virtuelle Azure Windows-Maschine die Anforderungen für die Installation des SnapCenter-Servers erfüllt. Weitere Informationen finden Sie unter "Bereiten Sie sich auf die Installation des SnapCenter-Servers vor".
- Wenn Sie neu bei Azure NetApp Files sind und noch kein NetApp-Konto besitzen, stellen Sie sicher, dass Sie sich registriert haben, damit Sie auf die SnapCenter-Software zugreifen können.

Schritte

1. Laden Sie das Installationspaket für den SnapCenter-Server von herunter "NetApp Support-Website".
2. Starten Sie die Installation des SnapCenter-Servers, indem Sie auf die heruntergeladene .exe-Datei doppelklicken.

   Nachdem Sie die Installation gestartet haben, werden alle Vorabprüfungen 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 werden.

3. Überprüfen Sie die für die SnapCenter Server-Installation erforderlichen vordefinierten Werte, und ändern Sie sie, falls erforderlich.

   Sie müssen das Kennwort für die MySQL Server Repository-Datenbank nicht angeben. Während der Installation des SnapCenter Servers wird das Passwort 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**.

   Wenn Sie ungültige Werte angegeben haben, werden entsprechende Fehlermeldungen angezeigt. Geben Sie die Werte erneut ein, und starten Sie dann die Installation.

   Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wird der ausgeführte Schritt abgeschlossen und der Rollback-Vorgang gestartet. Der SnapCenter-Server wird vollständig vom Host entfernt.

   Wenn Sie jedoch **Abbrechen** klicken, wenn die Vorgänge „Neustart des SnapCenter-Servers“ oder „Warten auf Start des SnapCenter-Servers“ ausgeführt werden, wird die Installation ohne Abbrechen des Vorgangs fortgesetzt.

Registrieren Sie das Produkt, um den Support zu aktivieren

Wenn Sie zum ersten mal bei NetApp sind und noch kein NetApp Konto haben, sollten Sie das Produkt registrieren, um den Support zu aktivieren.

Schritte

1. Navigieren Sie nach der Installation von SnapCenter zu **Hilfe > Info**.
2. Notieren Sie sich im Dialogfeld *Info zu SnapCenter* die SnapCenter-Instanz, eine 20-stellige Zahl, die mit 971 beginnt.
3. Klicken Sie Auf https://register.netapp.com.
4. Klicken Sie auf **Ich bin kein registrierter NetApp-Kunde**.

5. Geben Sie Ihre Daten an, um sich zu registrieren.
6. Lassen Sie das Feld NetApp Referenz SN leer.
7. Wählen Sie in der Dropdown-Liste Produktreihe **SnapCenter** aus.
8. Wählen Sie den Abrechnungsanbieter aus.
9. Geben Sie die 20-stellige SnapCenter-Instanz-ID ein.
10. Klicken Sie Auf **Absenden**.

Erstellen Sie die Azure-Zugangsdaten in SnapCenter

Sie sollten die Azure-Anmeldeinformationen in SnapCenter erstellen, um auf das Azure NetApp-Konto zuzugreifen.

Stellen Sie vor dem Erstellen der Azure-Anmeldeinformationen sicher, dass Sie den Dienstprinzipal in Azure erstellt haben. Zum Erstellen der Azure-Zugangsdaten müssen die Mandanten-ID, die Client-ID und der geheime Schlüssel, die dem Service-Principal zugeordnet sind, angegeben werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
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…	Tun Sie das…
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldedaten ein.
Authentifizierungsmodus	Wählen Sie **Azure Credential** aus der Dropdown-Liste aus.
Mandanten-ID	Geben Sie die Mandanten-ID ein.
Client-ID	Geben Sie die Client-ID ein.
Geheimer Client-Schlüssel	Geben Sie den geheimen Client-Schlüssel ein.

5. Klicken Sie auf **OK**.

Konfigurieren Sie das Azure Storage-Konto

Sie sollten das Azure Storage-Konto in SnapCenter konfigurieren.

Das Azure Storage-Konto enthält Details zu Abonnement-ID, Azure Zugangsdaten und Azure NetApp Konto.

Für Azure NetApp Files sind keine Standardlizenzen und kapazitätsbasierte Lizenz 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 Zugangsdaten, die Abonnement-ID und das NetApp-Konto in den entsprechenden Dropdown-Listen aus.
4. Klicken Sie Auf **Absenden**.

Erstellen Sie die Anmeldeinformationen, um den Plug-in-Host hinzuzufügen

SnapCenter verwendet Zugangsdaten, um Benutzer für SnapCenter-Vorgänge zu authentifizieren.

Sie sollten Anmeldedaten für die Installation von SnapCenter-Plug-ins und zusätzliche Anmeldedaten für die Durchführung von Datensicherungsvorgängen erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.
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…	**Tun Sie das…**
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldedaten ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus der Dropdown-Liste aus.
Authentifizierungstyp	Wählen Sie entweder **passwortbasiert** oder **SSH Key basiert** (nur für Linux-Host).
Benutzername	Geben Sie den Benutzernamen an.
Passwort	Wenn Sie die passwortbasierte Authentifizierung ausgewählt haben, geben Sie das Kennwort an.
Privater SSH-Schlüssel	Wenn Sie SSH Key Based Authentication ausgewählt haben, geben Sie den privaten Schlüssel an.
Sudo-Berechtigungen verwenden	Aktivieren Sie das Kontrollkästchen Sudo-Berechtigungen verwenden, wenn Sie Anmeldeinformationen für einen Benutzer ohne Root erstellen. Dies gilt nur für Linux-Benutzer.

5. Klicken Sie auf **OK**.

Schutz von SAP HANA Datenbanken

Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die SAP HANA Datenbank

Sie müssen Hosts über die Seite SnapCenter Add Host hinzufügen hinzufügen und dann die Plug-ins-Pakete installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Bevor Sie beginnen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.
- Wenn Sie auf dem zentralen Host installieren, 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. Vergewissern Sie sich, dass die Registerkarte **verwaltete Hosts** ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:
   a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
   b. Geben Sie im Feld Hostname den vollständig qualifizierten Domänennamen (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 Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Klicken Sie Auf **Absenden**.
8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und Senden**.

   In einer Cluster-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

9. Überwachen Sie den Installationsfortschritt.

Fügen Sie die SAP HANA-Datenbank hinzu

Sie sollten die SAP HANA-Datenbank manuell hinzufügen.

Über diese Aufgabe

Ressourcen müssen manuell hinzugefügt werden, wenn das Plug-in auf einem zentralen Server installiert ist. Wenn das SAP HANA-Plug-in auf dem HANA-Datenbank-Host installiert ist, wird das HANA-System

automatisch erkannt.

Die automatische Erkennung wird für die HANA-Konfiguration mit mehreren Hosts nicht unterstützt, sondern muss nur über ein zentralisiertes Plug-in hinzugefügt werden.

Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter-Plug-in für 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 bereitstellen“ die folgenden Aktionen durch:
   a. Geben Sie den Ressourcentyp entweder als Single Container, Multimandant Database Container oder Non-Data Volume 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 für die Verbindung zum SAP HANA-System ein.
   f. Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist.
4. Wählen Sie auf der Seite Speicher bereitstellen die Option **Azure NetApp Files** als Speichertyp aus.
   a. Wählen Sie das Azure NetApp Konto aus.
   b. Wählen Sie den Kapazitäts-Pool und die zugehörigen Volumes aus.
   c. Klicken Sie Auf **Speichern**.
5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Backup-Richtlinien für SAP HANA Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden, müssen Sie eine Backup-Richtlinie 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 Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Richtlinientyp die folgenden Schritte durch:
   a. Wählen Sie **Azure NetApp Files** als Speichertyp aus.
   b. Wählen Sie **dateibasiert**, wenn Sie eine Integritätsprüfung der Datenbank durchführen möchten.
   c. Wählen Sie **Snapshot-basiert**, wenn Sie ein Backup mit Snapshot-Technologie erstellen möchten.
6. Führen Sie auf der Seite Snapshot und Backup die folgenden Schritte durch:
   a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
   b. Legen Sie die Aufbewahrungseinstellungen fest.

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 stellen**.

Ressourcengruppen erstellen und SAP HANA Backup-Richtlinien anhängen

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags 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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, 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 Dropdown-Liste aus.
   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf * * für die Richtlinie, die Sie konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.
7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Sichern Sie auf Azure NetApp Files ausgeführte SAP HANA-Datenbanken

Wenn eine Ressource noch nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **Ansicht** nach Ressourcentyp.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Seite Ressource **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:
   a. Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen.
   b. Wählen Sie den Pfeil von **Scripts** aus, um Pre- und Post-Befehle für Stilllegung-, Snapshot- und Unquiesce-Vorgänge auszuführen.
   c. Wählen Sie den Pfeil **Custom Configurations** aus, und geben Sie dann die für alle Jobs, die diese Ressource verwenden, erforderlichen benutzerdefinierten Wertpaare ein.
   d. Wählen Sie **Snapshot-Kopierwerkzeug > SnapCenter ohne Dateisystemkonsistenz**, um Snapshots zu erstellen.

      Die Option **File System Consistency** gilt nur für Anwendungen, 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 Dropdown-Liste aus.
   b. Wählen Sie * *  in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy *Policy_Name* 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 Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.
8. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
9. Wählen Sie **Jetzt sichern**.
10. Führen Sie auf der Seite Backup die folgenden Schritte aus:
    a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

11. Wählen Sie **Backup**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Backup von SAP HANA-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **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 Backup die folgenden Schritte aus:
   a. Wenn der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für das Backup verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Wiederherstellung von SAP HANA Datenbanken

Sie können Daten aus den Backups wiederherstellen und wiederherstellen.

Über diese Aufgabe

Wenn für automatisch erkannte HANA-Systeme die Option **Complete Resource** ausgewählt ist, wird die Wiederherstellung mithilfe der Single File Snapshot-Wiederherstellungstechnologie durchgeführt. Wenn das Kontrollkästchen * Fast Restore* aktiviert ist, wird die Volume Revert-Technologie verwendet.

Für manuell hinzugefügte Ressourcen wird die Volume Revert-Technologie immer 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 **Ansicht** nach Ressourcentyp.
3. Wählen Sie die Ressource aus, oder wählen Sie eine Ressourcengruppe aus, und wählen Sie dann eine Ressource in dieser Gruppe aus.

4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option **Backups** aus den primären oder sekundären (gespiegelten oder ausgelagerten) Speichersystemen aus.
5. Wählen Sie in der Tabelle Primäres Backup(s) das Backup aus, das Sie wiederherstellen möchten, und klicken Sie dann auf * *  .
6. Wählen Sie auf der Seite Wiederherstellungsbereich die Option **komplette Ressource** aus.

   Alle konfigurierten Datenvolumes der SAP HANA-Datenbank werden wiederhergestellt.

7. Führen Sie für automatisch ermittelte HANA-Systeme auf der Seite Wiederherstellungsumfang die folgenden Aktionen durch:
   a. Wählen Sie **in den letzten Zustand wiederherstellen**, wenn Sie so nah wie möglich an der aktuellen Zeit wiederherstellen möchten.
   b. Wählen Sie **Recover to Point in Time** aus, wenn Sie sich an den angegebenen Zeitpunkt wiederherstellen möchten.
   c. Wählen Sie **Recover to specified Data Backup**, wenn Sie eine bestimmte Datensicherung wiederherstellen möchten.
   d. Wählen Sie **Keine Erholung**, wenn Sie jetzt nicht wiederherstellen möchten.
   e. Geben Sie die Speicherorte für die Protokollsicherung an.
   f. Geben Sie den Speicherort des Backup-Katalogs an.
8. Geben Sie auf der Seite Pre OPS die Befehle vor dem Wiederherstellen ein und heben Sie sie ab, bevor Sie einen Wiederherstellungsauftrag ausführen.
9. Geben Sie auf der Seite Post OPS Mount- und Post-Restore-Befehle ein, die ausgeführt werden sollen, nachdem eine Wiederherstellung durchgeführt wurde.
10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

    Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch auf der Seite **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Klonen des SAP HANA Datenbank-Backups

Sie können SnapCenter verwenden, um eine SAP HANA-Datenbank mit dem Backup der Datenbank zu klonen. Die erstellten Klone sind Thick Clones und werden im übergeordneten Kapazitätspool erstellt.

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 **Ansicht** nach Ressourcentyp.
3. Wählen Sie die Ressource oder Ressourcengruppe aus.
4. Wählen Sie in der Ansicht Manage Copies die Option **Backups** aus dem primären Speichersystem aus.

5. Wählen Sie die Datensicherung aus der Tabelle aus, und klicken Sie dann auf  .
6. Führen Sie auf der Seite Standort die folgenden Aktionen durch:

    a. Wählen Sie den Host aus, auf dem das SAP HANA-Plug-in zur Verwaltung des geklonten HANA-Systems installiert ist.

    Es kann ein zentralisierter Plug-in-Host oder HANA-System-Host sein.

    > Wenn das HANA-Plug-in auf einem zentralen Host installiert ist, der HANA-Datenbanken auf anderen Hosts verwaltet, während Klone erstellt oder gelöscht werden, überspringt SnapCenter bewusst Host-seitige Vorgänge (Dateisystem mounten oder unmounten), da der Zielserver ein zentralisierter Host ist. Sie sollten benutzerdefinierte Pre- oder Post-Clone-Skripte verwenden, um Mount- und Unmounting-Vorgänge auszuführen.

    a. Geben Sie den SAP HANA SID ein, um von den vorhandenen Backups zu klonen.
    b. Geben Sie IP-Adressen oder Hostnamen ein, auf denen die geklonten Volumes exportiert werden.
    c. Wenn die ANF-Volumes der SAP HANA-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie die QOS für die geklonten Volumes an.

    Wenn keine QOS für die geklonten Volumes angegeben wird, wird die QOS des Quell-Volume 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 den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.
    b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einen Host zu mounten.

    Wird das HANA-Quellsystem automatisch erkannt und das Clone-Ziel-Host-Plug-in auf dem SAP HANA-Host installiert, hängt SnapCenter die bestehenden HANA-Daten-Volumes auf dem Clone-Ziel-Host automatisch ab und mountet die neu geklonten HANA-Daten-Volumes.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

> Clone Split ist für ANF-Klone deaktiviert, da ANF-Klon bereits ein unabhängiges Volume ist, das aus dem ausgewählten Snapshot erstellt wird.

Microsoft SQL Server Datenbanken schützen

Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die SQL Server-Datenbank

SnapCenter unterstützt die Datensicherung von SQL-Instanzen auf SMB-Freigaben auf Azure NetApp Files. Die Standalone- und Verfügbarkeitsgruppen-Konfigurationen werden unterstützt.

Sie müssen die Seite SnapCenter Host hinzufügen verwenden, um Hosts hinzuzufügen, und dann das Plug-ins-Paket installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Bevor Sie beginnen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.

Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:
   a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
   b. Geben Sie im Feld Hostname den vollständig qualifizierten Domänennamen (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 **Plug-ins zur Installation 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 **Configure log Directory** und geben Sie auf der Seite Configure Host log Directory den SMB-Pfad des Host-Protokollverzeichnisses ein, und klicken Sie auf **Save**.
9. Klicken Sie auf **Absenden** und überwachen Sie den Installationsfortschritt.

Erstellen von Backup-Richtlinien 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. Alternativ können Sie beim Erstellen einer Ressourcengruppen oder beim Sichern einer einzelnen Ressource eine Backup-Richtlinie erstellen.

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 Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Richtlinientyp die folgenden Schritte durch:
   a. Wählen Sie **Azure NetApp Files** als Speichertyp aus.
   b. Wählen Sie den Sicherungstyp aus.
      i. Wählen Sie **Full Backup and Log Backup** aus, wenn Sie Datenbankdateien und Transaktionsprotokolle sichern möchten.
      ii. Wählen Sie **Full Backup**, wenn Sie nur die Datenbankdateien sichern möchten.

iii. Wählen Sie **Log Backup**, wenn Sie nur die Transaktionsprotokolle sichern möchten.

iv. Wählen Sie **nur Backup kopieren**, wenn Sie Ihre Ressourcen mit einer anderen Anwendung sichern möchten.

c. Führen Sie im Abschnitt Einstellungen für Verfügbarkeitsgruppen die folgenden Aktionen durch:

i. Wählen Sie auf bevorzugtem Backup-Replikat sichern, wenn Sie nur auf dem Replikat sichern möchten.

ii. Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für das Backup aus.

iii. Wählen Sie die Backup-Priorität aus.

6. Führen Sie auf der Seite Snapshot und Backup die folgenden Schritte durch:

a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.

b. Legen Sie die Aufbewahrungseinstellungen abhängig vom ausgewählten Sicherungstyp fest.

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 Überprüfung die folgenden Schritte aus:

a. Wählen Sie im Abschnitt Überprüfung ausführen für folgende Backup-Pläne die Zeitplanhäufigkeit aus.

b. Führen Sie im Abschnitt Optionen für die Datenbankkonsistenzprüfung die folgenden Aktionen durch:

i. Wählen Sie **Beschränkung der Integritätsstruktur auf physische Struktur der Datenbank (PHYSICAL_ONLY)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um gerissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen.

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)** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen.

iv. Wählen Sie * nicht gruppierte Indizes (NOINDEX)* aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten.

Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.

v. Wählen Sie **Schränken Sie die Prüfungen ein und erhalten Sie die Sperren anstatt eine interne Datenbank Snapshot Kopie (TABLOCK)** zu verwenden, um die Überprüfungen zu begrenzen und Sperren anstelle eines internen Datenbank-Snapshots zu erhalten.

c. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss bestätigen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.

d. Geben Sie im Abschnitt **Verification Script settings** den Pfad und die Argumente des Vorskripts bzw. Postscript ein, die vor oder nach dem Verifizierungsvorgang ausgeführt werden sollen.

8. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von SQL-Backup-Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags 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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, 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 Dropdown-Liste aus.
   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf * * für die Richtlinie, die Sie konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.
   d. Wählen Sie den Microsoft SQL Server Scheduler aus.
7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Wählen Sie den Überprüfungsserver aus.
   b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf * * .
   c. Wählen Sie entweder **Verifizierung nach Backup ausführen** oder **geplante Verifizierung ausführen**.
   d. Klicken Sie auf **OK**.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Sichern Sie auf Azure NetApp Files laufende SQL Server Datenbanken

Wenn eine Ressource noch nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Bevor Sie beginnen

Sie sollten einen Load Balancer erstellen, wenn dem Azure Windows-Failover-Cluster keine Cluster-IP zugewiesen ist oder wenn er nicht über SnapCenter erreichbar ist. Die IP des Load Balancer sollte konfiguriert und vom SnapCenter-Server aus erreichbar sein.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressource aus der Dropdown-Liste Ansicht die Option **Datenbank**, **Instanz** oder **Verfügbarkeitsgruppe** aus.
3. Wählen Sie auf der Seite Ressource **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 Dropdown-Liste aus.
   b. Wählen Sie * * in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann **OK** aus.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

   d. Wählen Sie **Use Microsoft SQL Server Scheduler** aus, und wählen Sie dann die Scheduler-Instanz aus der Dropdown-Liste **Scheduler-Instanz** aus, die mit der Planungsrichtlinie verknüpft ist.
5. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Wählen Sie den Überprüfungsserver aus.
   b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf * * .
   c. Wählen Sie entweder **Verifizierung nach Backup ausführen** oder **geplante Verifizierung ausführen**.
   d. Klicken Sie auf OK.
6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy**

die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

b. Wählen Sie **nach Sicherung prüfen**.

c. Wählen Sie **Backup**.

10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Sichern Sie SQL Server-Ressourcengruppen

Sie können die Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **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 Backup die folgenden Schritte aus:
   a. Wenn der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für das Backup verwenden möchten.
   b. Wählen Sie nach dem Backup **Verify** aus, um das On-Demand-Backup zu überprüfen.
   c. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Stellen Sie SQL Server Datenbanken wieder her

Sie können SnapCenter verwenden, um gesicherte SQL Server-Datenbanken wiederherzustellen. Die Datenbankwiederherstellung ist ein mehrstufiger Prozess, der alle Daten und Protokollseiten aus einem angegebenen SQL Server-Backup in eine angegebene Datenbank kopiert.

Über diese Aufgabe

Sie sollten sicherstellen, dass die Zielinstanz für die Wiederherstellung mit einem Active Directory-Benutzer konfiguriert ist, der zur SMB ADActive Directory-Domäne gehört und über die Berechtigungen 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 konfiguriert werden, wobei der Active Directory-Benutzer über die erforderlichen Berechtigungen verfügt.

Wenn das Dienstkonto für die SnapCenter-Plug-in-Dienste kein Active Directory-Benutzer ist, ist bei der Wiederherstellung auf einem alternativen Host der Benutzer erforderlich, der die volle Kontrolle über die Quell-Volumes hat, damit er imitiert werden kann 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 entweder **Datenbank** oder **Ressourcengruppe** aus der Liste Ansicht aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht Manage Copies die Option **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 „Bereich wiederherstellen“ 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 Backups durchgeführt werden.
   b. Wählen Sie **Wiederherstellen der Datenbank auf einem alternativen Host**, wenn Sie möchten, dass die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt wird, auf dem Backups durchgeführt werden.
7. Wählen Sie auf der Seite „Recovery Scope“ eine der folgenden Optionen aus:
   a. Wählen Sie **Keine** aus, wenn Sie nur das vollständige Backup ohne Protokolle wiederherstellen müssen.
   b. Wählen Sie **Alle Protokollsicherungen** Up-to-the-minute Backup Restore Operation, um alle verfügbaren Protokollsicherungen nach dem vollständigen Backup wiederherzustellen.
   c. Wählen Sie **nach Log-Backups**, um einen Point-in-Time-Wiederherstellungsvorgang durchzuführen, der die Datenbank basierend auf Backup-Protokollen bis zum ausgewählten Datum wiederherstellt.
   d. Wählen Sie **nach einem bestimmten Datum bis**, um Datum und Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht auf die wiederhergestellte Datenbank angewendet werden.
   e. Wenn Sie **Alle Log-Backups**, **durch Log-Backups** oder **nach einem bestimmten Datum bis** ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie **Benutzerdefiniertes Log-Verzeichnis verwenden** und geben Sie dann den Speicherort an.
8. Geben Sie auf der Seite Pre-Ops und Post Ops die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs**.

Klonen Sie das SQL Server Datenbank-Backup

Sie können SnapCenter verwenden, um eine SQL-Datenbank mithilfe des Backups der Datenbank zu klonen. Die erstellten Klone sind Thick Clones und werden im übergeordneten Kapazitätspool erstellt.

Über diese Aufgabe

Sie sollten sicherstellen, dass die Zielinstanz für den Klon mit einem Active Directory-Benutzer konfiguriert ist, der zur SMB ADActive Directory-Domäne gehört und über die Berechtigungen 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 konfiguriert werden, wobei der Active Directory-Benutzer über die erforderlichen

Berechtigungen verfügt.

Wenn das Dienstkonto für die SnapCenter-Plug-in-Dienste kein Active Directory-Benutzer ist, ist während des Klonens der Benutzer erforderlich, der die volle Kontrolle über die Quell-Volumes hat, damit er imitiert werden kann und den erforderlichen Vorgang ausführen kann.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Manage Copies** das Backup vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus, und wählen Sie dann * *  .
6. Geben Sie auf der Seite **Clone Options** alle erforderlichen Details an.
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 keine QOS für die geklonten Volumes angegeben wird, wird die QOS des Quell-Volume 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 **None**, wenn Sie nur die vollständige Sicherung ohne Protokolle klonen möchten.
   b. Wählen Sie **Alle Protokollsicherungen** aus, wenn Sie alle verfügbaren Protokollsicherungen klonen möchten, die nach dem vollständigen Backup datiert wurden.
   c. Wählen Sie **by log Backups until** aus, wenn Sie die Datenbank auf Basis der Backup-Protokolle klonen möchten, die bis zum Backup-Protokoll mit dem ausgewählten Datum erstellt wurden.
   d. Wählen Sie **nach spezifischem Datum bis** aus, wenn Sie die Transaktionsprotokolle nicht nach dem angegebenen Datum und der angegebenen Uhrzeit anwenden möchten.
9. Geben Sie auf der Seite **Script** das Skript-Timeout, den Pfad und die Argumente des Prescript oder Postscript ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
11. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Führen Sie Den Klon-Lebenszyklus Durch

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 ein Backup regelmäßig klonen, können Sie mit dem Klon Applikationen entwickeln, Daten ausfüllen oder Daten wiederherstellen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-

in aus der Liste aus.

2. Wählen Sie auf der Seite Ressourcen die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Manage Copies** das Backup vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus, und wählen Sie dann * *  .
6. Geben Sie auf der Seite **Clone Options** alle erforderlichen Details an.
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 keine QOS für die geklonten Volumes angegeben wird, wird die QOS des Quell-Volume verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Geben Sie auf der Seite **Script** das Skript-Timeout, den Pfad und die Argumente des Prescript oder Postscript ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
9. Führen Sie auf der Seite Zeitplan eine der folgenden Aktionen durch:
   - Wählen Sie **Jetzt ausführen** aus, wenn Sie den Klon-Job sofort ausführen möchten.
   - Wählen Sie **Configure schedule** aus, wenn Sie bestimmen möchten, wie häufig der Klonvorgang stattfinden soll, wann der Klonzeitplan starten soll, an welchem Tag der Klonvorgang stattfinden soll, wann der Zeitplan abläuft und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
11. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Schutz von Oracle Datenbanken

Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die Oracle-Datenbank

Auf der Seite „Host hinzufügen“ können Sie Hosts hinzufügen, und dann das SnapCenter Plug-ins Paket für Linux oder SnapCenter Plug-ins Package für AIX installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Sie können einen Host hinzufügen und Plug-in-Pakete für einen einzelnen Host oder für ein 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. Vergewissern Sie sich, dass die Registerkarte **verwaltete Hosts** ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.

4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:
   a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
   b. Geben Sie im Feld Hostname den vollständig qualifizierten Domänennamen (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 Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Klicken Sie Auf **Absenden**.
8. Überprüfen Sie den Fingerabdruck, und klicken Sie dann auf **Bestätigen und Senden**.

   In einer Cluster-Einrichtung sollten Sie den Fingerabdruck aller Nodes im Cluster überprüfen.

9. Überwachen Sie den Installationsfortschritt.

Erstellung von Backup-Richtlinien für Oracle Datenbanken

Bevor Sie SnapCenter zum Backup von Oracle-Datenbankressourcen verwenden, müssen Sie eine Backup-Richtlinie 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 Database aus der Dropdown-Liste aus.
4. Klicken Sie Auf **Neu**.
5. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
6. Führen Sie auf der Seite Richtlinientyp die folgenden Schritte durch:
   a. Wählen Sie **Azure NetApp Files** als Speichertyp aus.
   b. Wählen Sie den Sicherungstyp als Online- oder Offline-Backup aus.
   c. Wenn Sie das Backup mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Katalog-Backup mit Oracle Recovery Manager (RMAN)** aus.
   d. Wenn Sie Archivprotokolle nach Backup beschneiden möchten, wählen Sie **Prune Archivprotokolle nach Backup** aus.
   e. Geben Sie die Einstellungen für das Archivprotokoll zum Löschen an.
7. Führen Sie auf der Seite Snapshot und Backup die folgenden Schritte durch:
   a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
   b. Legen Sie die Aufbewahrungseinstellungen fest.
   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 Prescript oder Postscript ein, das Sie vor oder nach dem Backup ausführen möchten.
9. Wählen Sie auf der Seite Verifizierung den Backup-Zeitplan aus, für den Sie den Überprüfungsvorgang durchführen möchten, und geben Sie den Pfad und die Argumente des Prescript- oder Postscript ein, das

Sie vor bzw. nach dem Überprüfungsvorgang ausführen möchten.

10. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Oracle-Backup-Richtlinien

Eine Ressourcengruppe ist der Container, dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags 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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.
Ziel der Archivprotokolldatei	Geben Sie die Ziele der Archivprotokolldateien an.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, 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 Dropdown-Liste aus.
   b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf * *  für die Richtlinie, die Sie konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.
7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Wählen Sie den Überprüfungsserver aus.

b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf * + .

c. Wählen Sie entweder **Verifizierung nach Backup ausführen** oder **geplante Verifizierung ausführen**.

d. Klicken Sie auf **OK**.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Sichern Sie auf Azure NetApp Files laufende Oracle Datenbanken

Wenn eine Ressource noch nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressource aus der Dropdown-Liste Ansicht die Option **Datenbank** aus.
3. Wählen Sie auf der Seite Ressource **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 Dropdown-Liste aus.
   b. Wählen Sie * * + in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann **OK** aus.
5. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Wählen Sie den Überprüfungsserver aus.
   b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf * * + .
   c. Wählen Sie entweder **Verifizierung nach Backup ausführen** oder **geplante Verifizierung ausführen**.
   d. Klicken Sie auf OK.
6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

b. Klicken Sie Auf **Backup**.

10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Erstellen Sie ein Backup von Oracle Ressourcengruppen

Sie können die Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, 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 **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 Backup die folgenden Schritte aus:
   a. Wenn der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für das Backup verwenden möchten.
   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Stellen Sie Oracle Datenbanken wieder her

Bei einem Datenverlust können Sie mit SnapCenter Daten von einem oder mehreren Backups auf Ihrem aktiven Dateisystem wiederherstellen und dann 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 entweder **Datenbank** oder **Ressourcengruppe** aus der Liste Ansicht aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht Manage Copies die Option **Backups** aus dem primären Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf * *  .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wählen Sie RAC aus, wenn Sie ein Backup einer Datenbank in der RAC-Umgebung ausgewählt haben.
   b. Führen Sie folgende Aktionen durch:
      i. Wählen Sie **Alle Datendateien** aus, wenn Sie nur die Datenbankdateien wiederherstellen möchten.
      ii. Wählen Sie **Tablespaces**, wenn Sie nur die Tablespaces wiederherstellen möchten.
      iii. Wählen Sie **Protokolldateien wiederholen** aus, wenn Sie die Redo-Protokolldateien der Data

Guard Standby- oder Active Data Guard-Standby-Datenbanken wiederherstellen möchten.

iv. Wählen Sie **Pluggable Databases** aus 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 Backups durchgeführt werden.

vii. Wählen Sie **Wiederherstellen der Datenbank auf einem alternativen Host**, wenn Sie möchten, dass die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt wird, auf dem Backups durchgeführt werden.

viii. Wählen Sie **Datenbankstatus ändern, falls erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.

ix. Wählen Sie **erzwingen in place Restore** aus, wenn Sie in den Szenarien, in denen neue Datendateien nach dem Backup hinzugefügt werden, oder wenn LUNs zu einer LVM-Laufwerksgruppe hinzugefügt, gelöscht oder neu erstellt werden sollen, in-place-Wiederherstellung durchführen möchten.

7. Wählen Sie auf der Seite „Recovery Scope“ 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 eine Wiederherstellung auf eine bestimmte SCN durchführen möchten.
   c. Wählen Sie **Datum und Uhrzeit**, wenn Sie sich auf ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten.
   d. Wählen Sie **Keine Wiederherstellung**, wenn Sie nicht wiederherstellen möchten.
   e. Wählen Sie **Geben Sie externe Archivprotokollspeicherorte an**, 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 Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Wiederherstellen von Tabellen mit Point-in-Time Recovery

Sie können eine Teilmenge an beschädigten oder abfallenen Tablespaces wiederherstellen, ohne die anderen Tablespaces in der Datenbank zu beeinträchtigen. SnapCenter verwendet RMAN für die Durchführung des Point-in-Time Recovery (PITR) der Tabellen.

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 Ansicht aus.
3. Wählen Sie die Datenbank des Typs Einzelinstanz (mandantenfähig) aus.

4. Wählen Sie aus der Ansicht Kopien verwalten im Speichersystem **Backups** aus.

   Wenn die Sicherung nicht katalogisiert ist, sollten Sie die Sicherung auswählen und auf **Katalog** klicken.

5. Wählen Sie die katalogisierte Sicherung aus, und klicken Sie dann auf * * .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wählen Sie **RAC** aus, wenn Sie ein Backup 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 erforderlich für Wiederherstellung und Wiederherstellung**, um den Status der Datenbank in den Zustand zu ändern, der für die Wiederherstellung und Wiederherstellung erforderlich ist.
7. Wählen Sie auf der Seite „Recovery Scope“ eine der folgenden Optionen aus:
   a. Wählen Sie **bis SCN (System Change Number)**, wenn Sie eine Wiederherstellung auf eine bestimmte SCN durchführen möchten.
   b. Wählen Sie **Datum und Uhrzeit**, wenn Sie sich auf ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten.
8. Geben Sie auf der Seite Pre-Ops und Post Ops die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs**.

Wiederherstellen steckbarer Datenbanken über zeitpunktgenaues Recovery

Sie können eine steckbare Datenbank (PDB) wiederherstellen, die beschädigt oder verworfen wurde, ohne die andere DBs in der Container-Datenbank (CDB) zu belasten. SnapCenter nutzt RMAN für die Durchführung von Point-in-Time Recoverys (PITR) der PDB.

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 Ansicht aus.
3. Wählen Sie die Datenbank des Typs Einzelinstanz (mandantenfähig) aus.
4. Wählen Sie aus der Ansicht Kopien verwalten im Speichersystem **Backups** aus.

   Wenn die Sicherung nicht katalogisiert ist, sollten Sie die Sicherung auswählen und auf **Katalog** klicken.

5. Wählen Sie die katalogisierte Sicherung aus, und klicken Sie dann auf * * .
6. Führen Sie auf der Seite „Wiederherstellungsumfang“ die folgenden Aufgaben durch:
   a. Wählen Sie **RAC** aus, wenn Sie ein Backup einer Datenbank in einer RAC-Umgebung ausgewählt haben.
   b. Je nachdem, ob Sie die PDB oder Tablespaces in einer PDB wiederherstellen möchten, führen Sie eine der folgenden Aktionen aus:

- Wählen Sie **Pluggable Databases (PDBs)** aus, 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 „Recovery Scope“ eine der folgenden Optionen aus:
   a. Wählen Sie **bis SCN (System Change Number)**, wenn Sie eine Wiederherstellung auf eine bestimmte SCN durchführen möchten.
   b. Wählen Sie **Datum und Uhrzeit**, wenn Sie sich auf ein bestimmtes Datum und eine bestimmte Uhrzeit wiederherstellen möchten.
8. Geben Sie auf der Seite Pre-Ops und Post Ops die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Monitor** > **Jobs**.

Klonen Sie das Backup von Oracle Datenbanken

Sie können SnapCenter verwenden, um eine Oracle Datenbank mithilfe des Backups der Datenbank zu klonen. Die erstellten Klone sind Thick Clones und werden im übergeordneten Kapazitätspool erstellt.

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 Ansicht aus.
3. Wählen Sie die Datenbank aus.
4. Wählen Sie auf der Seite „Manage Copies“ das Backup 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) klonen oder eine steckbare 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 die QOS für die geklonten Volumes an.

   Wenn keine QOS für die geklonten Volumes angegeben wird, wird die QOS des Quell-Volume 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 Credential Name for sys user die Credential aus, die zum Definieren des System-Benutzerpassworts der Clone-Datenbank verwendet werden soll.
   b. Wählen Sie für den Namen der ASM-Instanz Credential **None** aus, wenn die OS-Authentifizierung für die Verbindung mit der ASM-Instanz auf dem Clone-Host aktiviert ist.

      Wählen Sie andernfalls die Oracle ASM-Zugangsdaten aus, die entweder mit einem „sys“-Benutzer

oder einem Benutzer mit „sysasm“-Berechtigung für den Clone-Host konfiguriert sind.

9. Geben Sie auf der Seite Pre-Ops den Pfad und die Argumente der Verordnungen an und ändern Sie im Abschnitt Einstellungen für Datenbankparameter die Werte der vorinstallierten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
10. Auf der Post-Ops-Seite sind standardmäßig **Recover Database** und **until Cancel** ausgewählt, um die geklonte Datenbank wiederherzustellen.
    a. Wenn Sie **until Cancel** auswählen, führt SnapCenter die Wiederherstellung durch, indem es die letzte Protokollsicherung mit der ungebrochenen Sequenz von Archivprotokollen nach der Datensicherung, die zum Klonen ausgewählt wurde, einrichtet.
    b. Wenn Sie **Datum und Uhrzeit** auswählen, stellt SnapCenter die Datenbank bis zu einem bestimmten Datum und einer bestimmten Uhrzeit wieder her.
    c. Wenn Sie **until SCN** auswählen, stellt SnapCenter die Datenbank bis zu einem bestimmten SCN wieder her.
    d. Wenn Sie **externe Archivprotokollspeicherorte angeben** auswählen, identifiziert und hängt SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit ein.
    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 im externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.

    f. Aktivieren Sie das Kontrollkästchen * tempfile für temporären Tablespace erstellen*, wenn Sie ein tempfile für den temporären Standardtabulraum der geklonten Datenbank erstellen möchten.
    g. Fügen Sie in **Enter sql entries to apply when Clone is created** die sql-Einträge hinzu, die Sie anwenden möchten, wenn der Clone erstellt wird.
    h. Geben Sie unter **Enter Scripts to run after Clone Operation** den Pfad und die Argumente des Postscripts an, die Sie nach dem Clone-Vorgang ausführen möchten.
11. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
12. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
13. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Klonen einer sofort anschließbaren Datenbank

Sie können eine steckbare Datenbank (PDB) auf einem anderen oder demselben Ziel-CDB auf demselben Host oder einem anderen Host klonen. Sie können die geklonte PDB auch auf einem gewünschten SCN oder Datum und 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 entweder **Datenbank** oder **Ressourcengruppe** aus der Liste Ansicht aus.
3. Wählen Sie die Datenbank des Typs Einzelinstanz (mandantenfähig) aus.

4. Wählen Sie auf der Seite „Manage Copies“ das Backup vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus, und klicken Sie dann auf * *  .
6. Wählen Sie auf der Seite Name die Option **PDB Clone** aus, und geben Sie die weiteren 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 Verordnungen an und ändern Sie im Abschnitt Einstellungen für Datenbankparameter die Werte der vorinstallierten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
9. Auf der Post-Ops-Seite ist **until Cancel** standardmäßig ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.
    a. Wenn Sie **until Cancel** auswählen, führt SnapCenter die Wiederherstellung durch, indem es die letzte Protokollsicherung mit der ungebrochenen Sequenz von Archivprotokollen nach der Datensicherung, die zum Klonen ausgewählt wurde, einrichtet.
    b. Wenn Sie **Datum und Uhrzeit** auswählen, stellt SnapCenter die Datenbank bis zu einem bestimmten Datum und einer bestimmten Uhrzeit wieder her.
    c. Wenn Sie **externe Archivprotokollspeicherorte angeben** auswählen, identifiziert und hängt SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit ein.
    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 im externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.

    e. Aktivieren Sie das Kontrollkästchen * tempfile für temporären Tablespace erstellen*, wenn Sie ein tempfile für den temporären Standardtabulraum der geklonten Datenbank erstellen möchten.
    f. Fügen Sie in **Enter sql entries to apply when Clone is created** die sql-Einträge hinzu, die Sie anwenden möchten, wenn der Clone erstellt wird.
    g. Geben Sie unter **Enter Scripts to run after Clone Operation** den Pfad und die Argumente des Postscripts an, die Sie nach dem Clone-Vorgang ausführen möchten.
10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
11. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Management von SnapCenter Server und Plug-ins

Dashboard anzeigen

Überblick über das Dashboard

Im Navigationsbereich auf der linken Seite von SnapCenter erhalten Sie einen ersten Überblick über den Systemzustand Ihres Systems. Dazu gehören die letzten Jobaktivitäten, Warnmeldungen, Sicherungsübersicht, Storage-Effizienz und -Auslastung, der Status von SnapCenter Jobs (Backup, Klonen, Wiederherstellung), der Konfigurationsstatus für Standalone- und Windows-Cluster-Hosts. Anzahl von von SnapCenter gemanagten Storage Virtual Machines (SVMs) und Lizenzkapazität.

Die in der Dashboard-Ansicht angezeigten Informationen hängen von der Rolle ab, die dem Benutzer zugewiesen ist, der aktuell 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 mehr Informationen über ein Display anzeigen, indem Sie den Mauszeiger auf **i** bewegen. In manchen Fällen sind die Informationen in den Dashboard-Anzeigen mit detaillierten Quellinformationen auf SnapCenter-GUI-Seiten wie Ressourcen, Überwachung und Berichte verknüpft.

Zuletzt Verwendete Job-Aktivitäten

In der Kachel „Letzte Job-Aktivitäten“ werden die letzten Job-Aktivitäten von allen Backup-, Restore- und Clone-Jobs angezeigt, auf die Sie Zugriff haben. Jobs in dieser Anzeige haben einen der folgenden Status: Abgeschlossen, Warnung, Fehlgeschlagen, wird ausgeführt, Warteschlange, Und storniert.

Wenn Sie über einen Job fahren, erhalten Sie weitere Informationen. Sie können zusätzliche Jobinformationen anzeigen, indem Sie auf eine bestimmte Jobnummer klicken, die Sie zur Seite Überwachung umleitet. Dort können Sie Job-Details oder Protokollinformationen abrufen und einen für diese Aufgabe spezifischen Bericht erstellen.

Klicken Sie auf **Alle anzeigen**, um eine Historie aller SnapCenter-Jobs anzuzeigen.

Meldungen

Im Feld „Meldungen“ werden die neuesten nicht behobenen kritischen Warnmeldungen und Warnmeldungen für die Hosts und den SnapCenter-Server angezeigt.

Die Gesamtzahl der Warnmeldungen für kritische und Warnungskategorien wird oben auf dem Display angezeigt. Wenn Sie auf die Summen „kritisch“ oder „Warnung“ klicken, werden Sie zur Seite „Warnungen“ weitergeleitet, auf der der Seite „Meldungen“ der spezifische Filter angewendet wird.

Wenn Sie auf eine bestimmte Warnmeldung klicken, werden Sie zur Seite „Meldungen“ weitergeleitet, die Ihnen Details zu dieser Warnmeldung enthält. Wenn Sie unten auf der Anzeige auf **Alle anzeigen** klicken, werden Sie zur Seite Warnungen weitergeleitet, um eine Liste aller Warnmeldungen anzuzeigen.

Aktuelle Zusammenfassung Des Schutzes

Die Kachel Letzte Protection Summary gibt Ihnen den Schutzstatus für alle Einheiten an, auf die Sie Zugriff haben. Standardmäßig wird die Anzeige so eingestellt, dass der Status aller Plug-ins angezeigt wird. Statusinformationen werden für Ressourcen bereitgestellt, die im Primärspeicher als Snapshots gesichert werden, und für Sekundärspeicher mithilfe von SnapMirror und SnapVault Technologien. Die Verfügbarkeit von Schutzstatusinformationen für den sekundären Speicher basiert auf dem ausgewählten Plug-in-Typ.

Wenn Sie eine Mirror-Vault-Schutzrichtlinie verwenden, werden die Zähler für die Sicherungszusammenfassung im SnapVault-Übersichtsdiagramm und nicht im SnapMirror Diagramm angezeigt.

Der Schutzstatus für einzelne Plug-ins wird durch Auswahl eines Plug-ins im Dropdown-Menü angezeigt. Ein Donut-Diagramm zeigt den Prozentsatz der geschützten Ressourcen für das ausgewählte Plug-in. Wenn Sie auf ein Donut-Slice klicken, werden Sie zur Seite **Reports** > **Plug-in** weitergeleitet, die einen detaillierten Bericht über alle primären und sekundären Speicheraktivitäten für das angegebene Plug-in enthält.

Berichte über sekundären Storage gelten nur für SnapVault. SnapMirror Berichte werden nicht unterstützt.

SAP HANA bietet Informationen zum Sicherungsstatus für primären und sekundären Storage für Snapshots. Für dateibasierte Backups steht nur der Schutzstatus des primären Storage zur Verfügung.

Sicherungsstatus	Primärspeicher	Sekundär-Storage
Fehlgeschlagen	Anzahl der Einheiten, die Teil einer Ressourcengruppe sind, in der die Ressourcengruppe ein Backup ausgeführt hat, das Backup jedoch fehlgeschlagen ist.	Anzahl der Einheiten mit Backups, die nicht an ein sekundäres Ziel übertragen wurden.
Erfolgreich	Anzahl der Einheiten in einer Ressourcengruppe, in der die Ressourcengruppe erfolgreich gesichert wurde.	Anzahl der Einheiten mit Backups, die erfolgreich an ein sekundäres Ziel übertragen wurden.
Nicht konfiguriert	Anzahl der Einheiten, die nicht zu einer Ressourcengruppe gehören und noch nicht gesichert wurden.	Anzahl der Einheiten, die Teil einer oder mehrerer Ressourcengruppen sind, die nicht für Backups konfiguriert sind, die an ein sekundäres Ziel übertragen werden sollen.
Nicht initiiert	Anzahl der Einheiten, die Teil einer Ressourcengruppe sind, aber kein Backup ausgeführt wurde.	Keine Angabe.

Wenn Sie zum Erstellen von Backups SnapCenter Server 4.2 und eine frühere Version des Plug-ins (früher als 4.2) verwenden, wird der SnapMirror Sicherungsstatus dieser Backups im Kachel **Neueste Schutzzusammenfassung** nicht angezeigt.

Jobs

Die Kachel Jobs bietet Ihnen eine Zusammenfassung der Backup-, Wiederherstellungs- und Klonaufgaben, auf die Sie Zugriff haben. Sie können den Zeitrahmen für jeden Bericht über das Dropdown-Menü anpassen. Die Optionen für den Zeitrahmen werden in den letzten 24 Stunden, den letzten 7 Tagen und den letzten 30 Tagen festgelegt. Der Standardbericht zeigt die in den letzten 7 Tagen ausgeführten Datensicherungsaufträge an.

Jobinformationen zum Sichern, Wiederherstellen und Klonen werden in Donut-Diagrammen angezeigt. Wenn Sie auf eine Donut-Schicht klicken, werden Sie zur Seite „Monitor“ umgeleitet, auf der die Jobfilter bereits für die Auswahl angewendet werden.

Aufgabenstatus	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 aktuell ausgeführten Jobs.

Storage

Im Bereich Storage wird der primäre und sekundäre Storage, der von Sicherungsaufgaben über einen Zeitraum von 90 Tagen verbraucht wird, grafisch dargestellt und zeigt Verbrauchstrends berechnet. Die Speicherinformationen werden alle 24 Stunden um 12 Uhr aktualisiert

Der Tagesverbrauch, der die Gesamtzahl der in SnapCenter verfügbaren Backups und die durch diese Backups belegte Größe umfasst, wird oben auf dem Display angezeigt. Ein Backup könnte mehrere Snapshots zugeordnet haben, und die Anzahl wird die gleiche reflektieren. Dies gilt sowohl für primäre als auch für sekundäre Snapshots. Sie haben z. B. 10 Backups erstellt, von denen 2 aufgrund der richtlinienbasierten Backup-Aufbewahrung gelöscht werden und 1 Backup von Ihnen explizit gelöscht wird. Somit wird eine Anzahl von 7 Backups zusammen mit der Größe angezeigt, die von diesen 7 Backups belegt wird.

Der Storage-Einsparungsfaktor für Primär-Storage ist das Verhältnis der logischen Kapazität (Einsparungen durch Klone und Snapshots plus verbrauchter Storage) zur physischen Kapazität des primären Storage. Ein Balkendiagramm zeigt die Storage-Einsparungen.

Das Liniendiagramm stellt den primären und sekundären Speicherverbrauch über einen laufenden Zeitraum von 90 Tagen täglich separat dar. Wenn Sie über die Diagramme fahren, erhalten Sie detaillierte tägliche Ergebnisse.

Wenn Sie zum Erstellen von Backups SnapCenter Server 4.2 und eine frühere Version des Plug-ins (früher als 4.2) verwenden, werden im Kachel **Storage** nicht die Anzahl der Backups, der von diesen Backups benötigte Storage, die Snapshot-Einsparungen, die Kloneinsparungen und die Snapshot-Größe angezeigt.

Konfiguration

Die Konfigurationtile bietet konsolidierte Statusinformationen für alle aktiven eigenständigen und Windows Cluster Hosts, die SnapCenter verwaltet, und auf die Sie Zugriff haben. Dazu gehören auch die mit diesen Hosts verknüpften Plug-in-Statusinformationen.

Wenn Sie auf die Zahl neben Hosts klicken, werden Sie auf der Seite Hosts zum Abschnitt Managed Hosts umgeleitet. Von dort erhalten Sie detaillierte Informationen zu einem ausgewählten Host.

Zusätzlich zeigt dieses Display die Summe der eigenständigen ONTAP SVMs und Cluster ONTAP SVMs, die SnapCenter verwaltet und auf die Sie Zugriff haben. Wenn Sie auf die neben SVM angrenzende Zahl klicken, werden Sie zur Seite Storage-Systeme umgeleitet. Von dort erhalten Sie ausführliche Informationen zu einer ausgewählten SVM.

Der Status der Host-Konfiguration wird als rot (kritisch), gelb (Warnung) und grün (aktiv) angezeigt. Zudem wird die Anzahl der Hosts im jeweiligen Status angegeben. Für jeden Status werden Statusmeldungen bereitgestellt.

Konfigurationsstatus	Beschreibung
Upgrade erforderlich	Anzahl der Hosts, auf denen nicht unterstützte Plug-ins ausgeführt werden und ein Upgrade erforderlich ist Ein nicht unterstütztes Plug-in ist mit dieser SnapCenter-Version nicht kompatibel.
Migration erforderlich	Anzahl der Hosts, auf denen nicht unterstützte Plug-ins ausgeführt werden und Migration erforderlich ist Ein nicht unterstütztes Plug-in ist mit dieser SnapCenter-Version nicht kompatibel.
Es sind keine Plug-ins installiert	Anzahl der Hosts, die erfolgreich hinzugefügt, aber die Plug-ins müssen installiert werden, oder die Installation der Plug-ins ist fehlgeschlagen.
Ausgesetzt	Anzahl der Hosts, deren Zeitpläne ausgesetzt und gewartet werden.
Angehalten	Anzahl der Hosts, die in Betrieb sind, die Plug-in-Services jedoch nicht ausgeführt werden.
Host ausgefallen	Anzahl der Hosts, die ausgefallen sind oder nicht erreichbar sind.
Upgrade verfügbar (optional)	Anzahl der Hosts, auf denen eine neuere Version des Plug-in-Pakets zur Aktualisierung verfügbar ist.

Konfigurationsstatus	Beschreibung
Migration verfügbar (optional)	Anzahl der Hosts, auf denen eine neuere Version des Plug-ins für die Migration verfügbar ist
Protokollverzeichnis konfigurieren	Anzahl der Hosts, für die SCSQL das Protokollverzeichnis konfiguriert werden muss, um die Sicherung des Transaktionsprotokolls zu erstellen.
Konfiguration von VMware Plug-ins	Anzahl der Hosts, die das SnapCenter Plug-in für VMware vSphere hinzufügen müssen
Unbekannt	Anzahl der Hosts, die registriert wurden, aber die Installation noch nicht ausgelöst wurde.
Wird Ausgeführt	Anzahl der Hosts, die vorhanden sind und Plug-ins werden ausgeführt. Und bei SCSLL-Plug-ins werden Logverzeichnis und Hypervisor konfiguriert.
Installieren\Deinstallieren von Plug-ins	Anzahl der Hosts, auf denen Plug-in-Installation oder Deinstallation ausgeführt wird.

So zeigen Sie Informationen auf dem Dashboard an

Im linken Navigationsbereich der 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. Die in den einzelnen Displays bereitgestellten Inhalte hängen von der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) ab.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Klicken Sie auf die aktiven Bereiche der Anzeige, um weitere Informationen zu erhalten.

   Wenn Sie beispielsweise in **Jobs** auf ein Donut-Diagramm klicken, werden Sie zur Seite Überwachen umgeleitet, um weitere Informationen zu Ihrer Auswahl zu erhalten. Durch Klicken auf ein Donut-Diagramm in **Schutz-Übersicht** werden Sie zur Seite Berichte weitergeleitet, die Ihnen weitere Informationen zu Ihrer Auswahl geben kann.

Statusberichte der Jobs über das Dashboard anfordern

Sie können Berichte über Backup-, Wiederherstellungs- und Klonaufträge über die Dashboard-Seite 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 die Kachel Jobs und wählen Sie dann **Backup**, **Restore** oder **Clone** aus.
3. Wählen Sie im Pulldown-Menü den Zeitrahmen aus, für den Sie Jobinformationen wünschen: 24 Stunden, 7 Tage oder 30 Tage.

   Die Systeme zeigen ein Donut-Diagramm, das die Daten abdeckt.

4. Klicken Sie auf die Donut-Schicht, die die Jobinformationen enthält, für die Sie einen Bericht erstellen möchten.

   Wenn Sie auf das Donut-Diagramm klicken, werden Sie von der Dashboard-Seite zur Monitor-Seite umgeleitet. Auf der Seite „Überwachen“ werden die Jobs angezeigt, die den Status aufweisen, den Sie im Donut-Diagramm ausgewählt haben.

5. Klicken Sie in der Liste Monitor auf einen bestimmten Job, um ihn auszuwählen.
6. Klicken Sie oben auf der Monitor-Seite auf **Berichte**.

Ergebnis

Der Bericht zeigt nur Informationen für den ausgewählten Job an. Sie können den Bericht prüfen oder auf Ihr lokales System herunterladen.

Berichte zum Sicherungsstatus können über das Dashboard angefordert werden

Sie können Sicherungsdetails für Ressourcen anfordern, die von bestimmten Plug-ins gemanagt werden, über das Dashboard. Nur Daten-Backups werden als Zusammenfassung zu Datensicherung in Betracht gezogen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Suchen Sie im Dashboard die Kachel Letzte Schutzübersicht, und wählen Sie über das Pulldown-Menü ein Plug-in aus.

   Das Dashboard zeigt ein Donut-Diagramm für Ressourcen an, die im primären Speicher gesichert sind und, falls zutreffend, für das Plug-in, ein Donut-Diagramm für Ressourcen, die auf dem sekundären Speicher gesichert sind.

   > Datensicherungsberichte sind nur für bestimmte Plug-ins-Typen verfügbar. Das Festlegen von **Alle Plug-ins** wird nicht unterstützt.

3. Klicken Sie auf die Donut-Schicht, die den Status darstellt, für den ein Bericht erstellt werden soll.

   Wenn Sie auf das Donut-Diagramm klicken, werden Sie von der Dashboard-Seite zu den Berichten und dann zur Plug-in-Seite umgeleitet. Der Bericht zeigt nur den Status des ausgewählten Plug-ins an. Sie können den Bericht prüfen oder auf Ihr lokales System herunterladen.

   > Umleitung zur Seite Berichte für SnapMirror-Donut-Diagramm und dateibasiertes SAP HANA-Backup wird nicht unterstützt.

RBAC managen

SnapCenter ermöglicht Ihnen, Rollen, Benutzer und Gruppen zu ändern.

Ändern Sie eine Rolle

Sie können eine SnapCenter-Rolle ändern, um Benutzer oder Gruppen zu entfernen und die mit der Rolle verknüpften Berechtigungen zu ändern. Es ist besonders nützlich, Rollen zu ändern, wenn Sie die Berechtigungen einer ganzen Rolle ändern oder löschen möchten.

Bevor Sie beginnen

Sie müssen sich als „SnapCenterAdmin“-Rolle angemeldet haben.

Sie können die Berechtigungen für die SnapCenterAdmin-Rolle nicht ändern oder 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. Ändern Sie auf der Seite Rollendetails die Berechtigungen, oder heben Sie die Zuweisung der Mitglieder nach Bedarf ab.
5. Wählen Sie **Alle Mitglieder dieser Rolle können Objekte anderer Mitglieder** sehen, damit andere Mitglieder der Rolle nach der Aktualisierung der Ressourcenliste Ressourcen wie Volumes und Hosts sehen können.

   Deaktivieren Sie diese Option, wenn Mitglieder dieser Rolle keine Objekte anzeigen möchten, denen andere Mitglieder zugewiesen sind.

   Wenn diese Option aktiviert ist, ist es nicht erforderlich, Benutzern Zugriff auf Objekte oder Ressourcen zuzuweisen, wenn Benutzer derselben Rolle angehören wie der Benutzer, der die Objekte oder Ressourcen erstellt hat.

6. Klicken Sie Auf **Absenden**.

Benutzer und Gruppen ändern

Sie können SnapCenter-Benutzer oder -Gruppen ändern, um ihre Rollen und Assets zu ändern.

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 Sie ändern möchten.
4. Ändern Sie auf der Seite Benutzer- oder Gruppendetails die Rollen und Assets.

5. Klicken Sie Auf **Absenden**.

Management von Hosts

Sie können Hosts hinzufügen und SnapCenter-Plug-in-Pakete installieren, einen Verifizierungsserver hinzufügen, Hosts entfernen, Backup-Jobs migrieren und den Host aktualisieren, um Plug-in-Pakete zu aktualisieren oder neue Plug-in-Pakete hinzuzufügen. Abhängig vom verwendeten Plug-in können Sie auch Festplatten bereitstellen, SMB-Freigaben managen, Initiatorgruppen managen, iSCSI-Sessions managen und Daten migrieren.

Sie können diese Aufgaben ausführen…	**Für Microsoft Exchange Server**	**Für Microsoft SQL Server**	**Für Microsoft Windows**	**Für Oracle Database**	**Für SAP HANA Database**	**Für von NetApp unterstützte Plug-ins**	**Für Db2**	**Für PostgreSQL**	**Für MySQL**
Fügen Sie Hosts hinzu und installieren Sie das Plug-in-Paket	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Aktualisieren Sie ESXi-Informationen für einen Host	Nein	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Unterbrechen Sie die Zeitpläne und versetzen Sie Hosts in den Wartungsmodus	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 Database	Für SAP HANA Database	Für von NetApp unterstützte Plug-ins	Für Db2	Für PostgreSQL	Für MySQL
Ändern Sie Hosts durch Hinzufügen, Aktualisieren oder Entfernen von Plug-ins	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Entfernen Sie Hosts aus SnapCenter	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Starten Sie Plug-in-Services	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.
Bereitstellung von Festplatten	Nein	Nein	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
SMB-Freigaben managen	Nein	Nein	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
IGroups managen	Nein	Nein	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
Verwalten von iSCSI-Sitzungen	Nein	Nein	Ja.	Nein	Nein	Nein	Nein	Nein	Nein

Informationen zu Virtual Machines aktualisieren

Sie sollten Ihre Virtual Machine-Informationen aktualisieren, wenn sich die VMware vCenter-Anmeldedaten ändern oder der Datenbank- oder Dateisystem-Host neu startet. Durch die Aktualisierung der Informationen Ihrer Virtual Machine in SnapCenter wird die Kommunikation mit dem VMware vSphere vCenter initiiert und die Anmeldedaten für vCenter abgerufen.

RDM-basierte Festplatten werden vom SnapCenter-Plug-in für Microsoft Windows verwaltet, das auf dem Datenbank-Host installiert ist. Um RDMs zu managen, kommuniziert das SnapCenter Plug-in für Microsoft Windows mit dem vCenter Server, der den Datenbank-Host managt.

Schritte

1. Klicken Sie im linken Navigationsbereich des SnapCenter auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie auf der Seite verwaltete Hosts den Host aus, den Sie aktualisieren möchten.
4. Klicken Sie auf **VM aktualisieren**.

Ändern Sie die Plug-in-Hosts

Nach der Installation eines Plug-ins können Sie ggf. die Details der Plug-in Hosts ändern. Sie können Anmeldeinformationen, Installationspfad, Plug-ins, Logverzeichnis-Details für das SnapCenter-Plug-in für Microsoft SQL Server, das Group Managed Service Account (gMSA) und den Plug-in-Port ändern.

Stellen Sie sicher, dass die Plug-in-Version mit der Version des SnapCenter-Servers identisch ist.

Über diese Aufgabe

- Sie können einen Plug-in-Port erst ändern, nachdem das Plug-in installiert wurde.

  Sie können den Plug-in-Port nicht ändern, während Upgrade-Vorgänge ausgeführt werden.

- Beim Ändern eines Plug-in-Ports sollten Sie die folgenden Port-Rollback-Szenarien beachten:
  - Wenn SnapCenter in einem eigenständigen Setup den Port einer der Komponenten nicht ändert, schlägt der Vorgang fehl und der alte Port wird für alle Komponenten beibehalten.

    Wenn der Port für alle Komponenten geändert wurde, aber eine der Komponenten nicht mit dem neuen Port startet, wird der alte Port für alle Komponenten beibehalten. Wenn Sie beispielsweise den Port für zwei Plug-ins auf dem Standalone-Host ändern möchten und SnapCenter den neuen Port nicht auf eines der Plug-ins anwenden kann, schlägt der Vorgang fehl (mit entsprechender Fehlermeldung) und der alte Port wird für beide Plug-ins beibehalten.

  - Wenn SnapCenter in einer geclusterten Einrichtung den Port des auf einem Node installierten Plug-ins nicht ändert, schlägt der Vorgang fehl und der alte Port wird für alle Nodes beibehalten.

    Wenn beispielsweise das Plug-in auf vier Nodes in einem Cluster-Setup installiert ist und wenn der Port nicht für einen der Nodes geändert wird, wird der alte Port für alle Nodes beibehalten.

Wenn Plug-ins mit gMSA installiert sind, können Sie im Fenster **More Options** ändern. Wenn Plug-ins ohne

gMSA installiert sind, können Sie das gMSA-Konto angeben, um es als Plug-in-Dienstkonto zu verwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Vergewissern Sie sich, dass **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie den Host aus, für den Sie ein Feld ändern und ändern möchten.

   Es kann jeweils nur ein Feld geändert werden.

4. Klicken Sie Auf **Absenden**.

Ergebnis

Der Host wurde validiert und zum SnapCenter-Server hinzugefügt.

Plug-in-Dienste starten oder neu starten

Wenn Sie die SnapCenter Plug-in-Dienste starten, können Sie Dienste starten, wenn sie nicht ausgeführt werden, oder wenn sie ausgeführt werden. Sie möchten die Dienste möglicherweise neu starten, nachdem die Wartung durchgeführt wurde.

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 Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie auf der Seite verwaltete Hosts den Host aus, den Sie starten möchten.
4. Klicken Sie auf **Dienst starten** oder **Dienst neu starten**.

   Sie können den Service mehrerer Hosts gleichzeitig starten oder neu starten.

Unterbrechen Sie die Zeitpläne für die Hostwartung

Wenn Sie verhindern möchten, dass der Host geplante SnapCenter-Jobs ausführt, können Sie Ihren Host in den Wartungsmodus versetzen. Führen Sie dies vor dem Upgrade der Plug-ins durch oder führen Sie Wartungsaufgaben auf Hosts durch.

Sie können die Zeitpläne auf einem Host nicht unterbrechen, der ausgefallen ist, da SnapCenter nicht mit diesem Host kommunizieren kann.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie auf der Seite verwaltete Hosts den Host aus, den Sie aussetzen möchten.
4. Klicken Sie auf , und klicken Sie dann auf **Zeitplan unterbrechen**, um den Host für dieses Plug-in in den Wartungsmodus zu versetzen.

Sie können den Zeitplan mehrerer Hosts gleichzeitig unterbrechen.

Sie müssen den Plug-in-Dienst nicht zuerst beenden. Der Plug-in-Dienst kann sich im Status „ausgeführt“ oder „angehalten“ befinden.

Ergebnis

Nachdem Sie die Zeitpläne auf dem Host unterbrochen haben, wird auf der Seite Managed Hosts **suspended** im Feld Gesamtstatus des Hosts angezeigt.

Nachdem Sie die Host-Wartung abgeschlossen haben, können Sie den Host aus dem Wartungsmodus bringen, indem Sie auf **Zeitplan aktivieren** klicken. Sie können den Zeitplan mehrerer Hosts gleichzeitig aktivieren.

Von der Seite Ressourcen unterstützte Vorgänge

Sie können auf der Seite Ressourcen Ressourcen Ressourcen Ressourcen Ressourcen erkennen und Datensicherungsvorgänge durchführen. Die Operationen, die Sie durchführen können, unterscheiden sich je nach dem Plug-in, das Sie für das Management 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 Database	Für SAP HANA Database
Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind	Ja.	Ja.	Ja.	Ja.	Ja.
On-Demand Backup einer Ressource durchführen	Ja.	Ja.	Ja.	Ja.	Ja.
Restore aus Backups	Ja.	Ja.	Ja.	Ja.	Ja.
Backups klonen	Nein	Ja.	Ja.	Ja.	Ja.
Backup-Management	Ja.	Ja.	Ja.	Ja.	Ja.
Management von Klonen	Nein	Ja.	Ja.	Ja.	Ja.

Sie können diese Aufgaben ausführen…	Für Microsoft Exchange Server	Für Microsoft SQL Server	Für Microsoft Windows	Für Oracle Database	Für SAP HANA Database
Management von Richtlinien	Ja.	Ja.	Ja.	Ja.	Ja.
Storage-Verbindungen managen	Ja.	Ja.	Ja.	Ja.	Ja.
Mount-Backups	Nein	Nein	Nein	Ja.	Nein
Deaktivieren Sie das Mounten von Backups	Nein	Nein	Nein	Ja.	Nein
Details anzeigen	Ja.	Ja.	Ja.	Ja.	Ja.

Management von Richtlinien

Sie können Richtlinien von einer Ressource oder Ressourcengruppe trennen, ändern, löschen, anzeigen und kopieren.

Richtlinien ändern

Sie können die Replikationsoptionen, die Snapshot-Aufbewahrungseinstellungen, die Anzahl der Fehlerversuche oder die Skriptinformationen ändern, während eine Richtlinie mit einer Ressource oder Ressourcengruppe verbunden ist. Sie können den Terminplantyp (Häufigkeit) nur ändern, wenn Sie eine Richtlinie trennen.

Über diese Aufgabe

Das Ändern des Zeitplantyps in einer Richtlinie erfordert zusätzliche Schritte, da der SnapCenter-Server den Zeitplantyp nur dann registriert, wenn die Richtlinie an eine Ressource oder Ressourcengruppe angeschlossen ist.

Ihr Ziel ist	Dann…
Fügen Sie einen zusätzlichen Terminplantyp hinzu	Erstellen Sie eine neue Richtlinie, und fügen Sie sie an die erforderlichen Ressourcen oder Ressourcengruppen an. Wenn z. B. eine Ressourcengruppenrichtlinie nur stündliche Backups angibt und Sie auch tägliche Backups 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.

Ihr Ziel ist	Dann…
Entfernen oder ändern Sie einen Planungstyp	Führen Sie Folgendes aus: 1. Trennen Sie die Richtlinie von allen Ressourcen- und Ressourcengruppen, die diese Richtlinie verwenden. 2. Ändern Sie den Terminplantyp. 3. Hängen Sie die Richtlinie erneut an alle Ressourcen und Ressourcengruppen an. Wenn z. B. eine Richtlinie stündliche Backups angibt und Sie diese in tägliche Backups ändern möchten, müssen Sie zuerst die Richtlinie trennen.

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 stellen**.

Richtlinien trennen

Sie können Richtlinien jederzeit von einer Ressource oder Ressourcengruppe trennen, wenn diese Richtlinien nicht mehr den Datenschutz für die Ressourcen regeln sollen. Sie müssen eine Richtlinie trennen, bevor Sie sie löschen können oder bevor Sie den Terminplantyp ändern.

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 **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 aus der Dropdown-Liste das Häkchen neben den Richtlinien, die Sie entfernen möchten.
5. Nehmen Sie zusätzliche Änderungen an der Ressourcengruppe im Rest des Assistenten vor, und klicken Sie dann auf **Fertig stellen**.

Richtlinien löschen

Wenn Sie keine Richtlinien mehr benötigen, können Sie sie löschen.

Bevor Sie beginnen

Sie sollten die Richtlinie von Ressourcen- oder Ressourcengruppen trennen, wenn die Richtlinie mit einer Ressource oder Ressourcengruppe 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 ausführen.

Sie können die folgenden Aufgaben bezüglich 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 während der Änderung der Ressourcengruppe ändern. Wenn Sie jedoch den Terminplantyp ändern möchten, müssen Sie die Richtlinie ändern.

  Wenn Sie Ressourcen aus einer Ressourcengruppe entfernen, werden die in den Richtlinien, die derzeit der Ressourcengruppe zugeordnet sind, definierten Backup-Aufbewahrungseinstellungen weiterhin auf die entfernten Ressourcen angewendet.

- Erstellen Sie ein Backup einer Ressourcengruppe.
- Erstellen Sie einen Klon eines Backups.

  Sie können die Backups von SQL, Oracle, Windows Filesystemen, benutzerdefinierten Applikationen und SAP HANA Datenbankressourcen oder Ressourcengruppen klonen.

- Erstellen Sie einen Klon einer Ressourcengruppe.

  Dieser Vorgang wird nur für SQL-Ressourcengruppen (die nur Datenbanken enthalten) unterstützt. Sie können einen Zeitplan für das Klonen einer Ressourcengruppe konfigurieren (Klon-Lebenszyklus).

- Verhindern Sie, dass geplante Vorgänge in Ressourcengruppen gestartet werden.
- Löschen einer Ressourcengruppe.

Stoppen und fortsetzen Sie den Betrieb in Ressourcengruppen

Sie können geplante Vorgänge vorübergehend vom Starten einer Ressourcengruppe deaktivieren. Später können Sie diese Vorgänge 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 **Ansicht** die Option **Ressourcengruppe** aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie auf **Wartung**.
4. Klicken Sie auf **OK**.

Wenn Sie die Vorgänge der Ressourcengruppe, die Sie im Wartungsmodus ausgeführt haben, wieder aufnehmen möchten, wählen Sie die Ressourcengruppe aus und klicken Sie auf **Produktion**.

Löschen von Ressourcengruppen

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 manuell alle Klone löschen, die für eine der Ressourcen der Ressourcengruppe erstellt wurden. Sie können optional das Löschen aller Backups, Metadaten, Richtlinien und Snapshots erzwingen, die der Ressourcengruppe zugeordnet 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 in der Liste **Ansicht** die Option **Ressourcengruppe** aus.
3. Wählen Sie die Ressourcengruppe aus, und klicken Sie dann auf **Löschen**.
4. Optional: Aktivieren Sie das Kontrollkästchen **Backups löschen und Richtlinien trennen, die dieser Ressourcengruppe zugeordnet sind**, um alle Backups, Metadaten, Richtlinien und Snapshots zu entfernen, die der Ressourcengruppe zugeordnet sind.
5. Klicken Sie auf **OK**.

Backup-Management

Sie können Backups umbenennen und löschen. Sie können auch mehrere Backups gleichzeitig löschen.

Backups umbenennen

Sie können Backups umbenennen, wenn Sie einen besseren Namen angeben möchten, um die Suchfähigkeit 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt. Wenn die Ressourcen- oder Ressourcengruppe nicht für den Datenschutz konfiguriert ist, wird anstelle der Topologieseite der Schutzassistent angezeigt.

4. Wählen Sie aus der Ansicht Kopien verwalten aus den primären Speichersystemen **Backups** aus.

   Sie können die Backups, die sich auf dem sekundären Speichersystem befinden, nicht umbenennen.

Wenn Sie die Backups von Oracle-Datenbanken mithilfe von Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Backups nicht umbenennen.

5. Wählen Sie die Sicherung aus, und klicken Sie dann auf  .
6. Geben Sie im Feld **Backup unter** umbenennen einen neuen Namen ein und klicken Sie auf **OK**.

Backups löschen

Backups können gelöscht werden, wenn das Backup für andere Datensicherungsvorgänge nicht mehr benötigt wird.

Bevor Sie beginnen

Sie müssen die zugehörigen Klone gelöscht haben, bevor Sie ein Backup löschen.

Wenn ein Backup einer geklonten Ressource zugeordnet ist, können Sie das Backup 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.
4. Wählen Sie aus der Ansicht Kopien verwalten aus den primären Speichersystemen **Backups** aus.

   Sie können die Backups, die sich auf dem sekundären Speichersystem befinden, nicht löschen.
5. Wählen Sie die Sicherung aus, und klicken Sie dann auf  .

   Wenn Sie ein SAP HANA-Datenbankbackup löschen, werden auch die zugehörigen SAP HANA-Kataloge des Backups gelöscht.

   Wenn das letzte verbleibende Backup gelöscht wird, können die zugehörigen HANA-Katalogeinträge nicht gelöscht werden.
6. Klicken Sie auf **OK**.

   Wenn Sie einige veraltete Datenbank-Backups in SnapCenter haben, die keine entsprechenden Backups auf dem Speichersystem haben, müssen Sie den Befehl remove-smbackup verwenden, um diese veralteten Backup-Einträge zu bereinigen. Wenn die veralteten Backups katalogisiert wurden, werden sie von der Datenbank des Recovery-Katalogs entkatalogisiert.

Schutz entfernen

Durch Entfernen des Schutzes werden alle Backups gelöscht und alle Richtlinien entfernt. Bevor Sie den

Schutz entfernen, sollten Sie sicherstellen, dass die Backups nicht gemountet werden und dass keine Klone mit dem Backup 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.

4. Wählen Sie die Sicherung aus und klicken Sie auf **Schutz entfernen**.

Klone löschen

Klone können gelöscht werden, wenn Sie sie nicht mehr benötigen.

Über diese Aufgabe

Klone, die sich als Quelle für andere Klone fungieren, können nicht gelöscht werden.

Wenn die Produktionsdatenbank beispielsweise db1 ist, wird Datenbank-Klon1 aus Backup von db1 geklont und anschließend clone1 geschützt. Der Datenbankklone2 wird aus dem Backup von Klon1 geklont. Wenn Sie Klon1 löschen möchten, müssen Sie zuerst Klon2 löschen 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Ressource“ oder „Topologie der Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
5. Wählen Sie den Klon aus, und klicken Sie dann auf  .

   Wenn Sie SAP HANA-Datenbankklone löschen, führen Sie auf der Seite Klonen löschen die folgenden Aktionen aus:

   a. Geben Sie im Feld **Pre Clone delete** die Befehle ein, die ausgeführt werden sollen, bevor Sie den Klon löschen.
   b. Geben Sie im Feld **Unmount** den Befehl ein, um die Bereitstellung des Klons zu deaktivieren, bevor Sie den Klon löschen.
6. Klicken Sie auf **OK**.

Nach Ihrer Beendigung

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 Löschvorgangs von Applikationsklonen und vor dem Löschen des Dateisystems warten müssen.

Nachdem Sie den Wert des Parameters geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu.

Überwachen von Jobs, Zeitplänen, Ereignissen und Protokollen

Sie können den Fortschritt Ihrer Jobs überwachen, Informationen zu geplanten Jobs abrufen und Ereignisse und Protokolle auf der Seite Überwachen überprüfen.

Überwachen von Jobs

Sie können Informationen zu Backup-, Klon-, Wiederherstellungs- und Verifizierungsaufgaben von SnapCenter anzeigen. Sie können diese Ansicht nach Start- und Enddatum, Jobtyp, Ressourcengruppe, Richtlinie oder SnapCenter-Plug-in filtern. Sie können auch zusätzliche Details und Protokolldateien für bestimmte Jobs erhalten.

Sie können auch Jobs bezüglich SnapMirror und SnapVault Vorgängen überwachen.

> Sie können nur die Jobs überwachen, die Sie erstellt haben und die für Sie relevant sind, es sei denn, Sie sind SnapCenter-Administrator oder eine andere Superuser-Rolle zugewiesen.

Sie können die folgenden Aufgaben im Zusammenhang mit Überwachungsaufgaben ausführen:

- Überwachen Sie Backup-, Klon-, Wiederherstellungs- und Überprüfungsvorgänge.
- Job-Details und -Berichte anzeigen
- Einen geplanten Job stoppen.

Managen geplanter Backup-Jobs

Ab 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. So können Sie die Anzahl der Backups steuern, die basierend auf der Hardwarekonfiguration des Systems ausgeführt werden sollen.

Der Standardwert für **JobConcurrencyThreshold** ist 0 und ist deaktiviert. Wenn Sie während des geplanten Backup-Fensters einen Performance-Abfall beobachten, kann die Aktivierung durch Zuweisen eines Werts aktiviert werden.

> Wenn Sie **JobConcurrencyThreshold** aktivieren, um gleichzeitige Jobs zu verwalten, erlaubt SnapCenter Ihnen nicht, die Reihenfolge der Backups zu steuern und die Backups werden möglicherweise nicht gleichzeitig ausgelöst, wie im Zeitplan angegeben.

Schritte

1. Legen Sie den Wert des Parameters *JobConcurrencyThreshold* unter *C:\Programme\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config* fest.
2. Führen Sie das Recycling des SnapCenter-Anwendungspools durch, indem Sie auf IIS > Anwendungspools > SnapCenter > Neu starten klicken.
3. Starten Sie den SnapCenter-Webdienst neu, indem Sie auf IIS > Sites > SnapCenter > Neu starten klicken.

Veraltete Jobs verwalten

Veraltete Jobs werden durch Unterbrechungen in SnapCenter oder durch unsachgemäße Job-Updates erstellt. Ab Version SnapCenter 6.0.1 wird ein vordefinierter Zeitplan eingeführt, um diese veralteten Jobs, die mehr als 72 Stunden im System stecken bleiben, zu bereinigen. 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* unter *C:\Programme\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config* fest.
2. Führen Sie das Recycling des SnapCenter-Anwendungspools durch, indem Sie auf IIS > Anwendungspools > SnapCenter > Neu starten klicken.
3. Starten Sie den SnapCenter-Webdienst neu, indem Sie auf IIS > Sites > SnapCenter > Neu starten klicken.

Überwachung von Zeitplänen

Sie möchten möglicherweise aktuelle Zeitpläne anzeigen, um zu bestimmen, wann der Vorgang gestartet wird, wann er zuletzt ausgeführt wurde und wann er als Nächstes ausgeführt wird. Sie können auch den Host bestimmen, auf dem der Vorgang ausgeführt wird, sowie die Ressourcengruppe und die Richtlinieninformationen des Vorgangs.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Monitor auf **Zeitpläne**.
3. Wählen Sie die Ressourcengruppe und den Terminplantyp aus.
4. Zeigen Sie die Liste der geplanten Vorgänge an.

Monitoring 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. die Erstellung eines geplanten Backups. Möglicherweise möchten Sie Ereignisse anzeigen, um zu bestimmen, ob ein Vorgang, z. B. ein Backup- oder Wiederherstellungsvorgang, derzeit 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 das Backup abgeschlossen ist, wird

ein Ereignis „`Backup Complete`“ angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Monitor auf **Events**.
3. (Optional) Geben Sie im Feld Filter das Start- oder Enddatum, die Ereigniskategorie (z. B. Backup, Ressourcengruppe oder Richtlinie) und den Schweregrad ein, und klicken Sie auf **Anwenden**. Alternativ können Sie auch Zeichen in das Suchfeld eingeben.
4. Zeigen Sie die Liste der Ereignisse an.

Monitoring von Protokollen

Sie können SnapCenter-Serverprotokolle, SnapCenter-Host-Agent-Protokolle und Plug-in-Protokolle anzeigen und herunterladen. Sie sollten die Protokolle anzeigen, die Ihnen bei der Fehlerbehebung helfen.

Über diese Aufgabe

Sie können die Protokolle filtern, um nur einen bestimmten Schweregrad für das Protokoll anzuzeigen:

- Debuggen
- Info
- Warnen
- Fehler
- Tödlich

Sie können auch Protokolle auf Jobebene abrufen, z. B. Protokolle, die Ihnen dabei helfen, den Grund für einen fehlgeschlagbaren Backup-Job zu beheben. 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 Ordner mit gezippten Daten enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des gezippten Ordners enthält die Job-id und den ausgewählten Jobtyp.

3. Klicken Sie auf der Seite Monitor auf **Protokolle**.
4. Wählen Sie Protokolltyp, Host und Instanz aus.

   Wenn Sie den Logtyp als **Plugin** auswählen, können Sie ein Host- oder SnapCenter-Plug-in auswählen. Dies ist nicht möglich, wenn der Logtyp **Server** ist.

5. Um die Protokolle nach einer bestimmten Quell-, Nachrichten- oder Protokollebene zu filtern, klicken Sie oben in der Spaltenüberschrift auf das Filtersymbol.

   Um alle Protokolle anzuzeigen, wählen Sie **größer als oder gleich** als `Debug` Level.

6. Klicken Sie Auf **Aktualisieren**.

7. Zeigen Sie die Liste der Protokolle an.
8. Klicken Sie auf **Download**, um die Protokolle herunterzuladen.

   Der heruntergeladene Ordner mit gezippten Daten enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des gezippten Ordners enthält die Job-id und den ausgewählten Jobtyp.

In großen Konfigurationen für eine optimale Performance sollten Sie die Protokolleinstellungen für SnapCenter mit dem PowerShell Cmdlet auf ein minimales Level setzen.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

Um nach Abschluss eines Failover-Jobs auf Integrations- oder Konfigurationsinformationen zuzugreifen, führen Sie das Cmdlet `Get-SmRepositoryConfig`aus.

Entfernen Sie Jobs und Protokolle aus SnapCenter

Sie können Backup-, Restore-, Klon- und Verifizierungsaufgaben und Protokolle aus SnapCenter entfernen. SnapCenter speichert erfolgreiche und fehlgeschlagene Job-Protokolle unbeschränkt, es sei denn, Sie entfernen sie. Möglicherweise möchten Sie sie entfernen, um den Storage aufzufüllen.

Über diese Aufgabe

Derzeit dürfen keine Jobs in Betrieb sein. Sie können einen bestimmten Job entfernen, indem Sie eine Job-ID angeben oder 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 an der Eingabeaufforderung Folgendes ein: `Open-SMConnection`
3. Geben Sie an 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.

Verwandte Informationen

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Überblick über die Berichterstellungsfunktionen von SnapCenter

SnapCenter bietet eine Vielzahl von Berichtsoptionen, mit denen Sie den Systemzustand und den Betrieb überwachen und managen können.

Berichtstyp	Beschreibung
Backup-Bericht	Der Backup-Bericht enthält allgemeine Daten zu Backup-Trends für Ihre SnapCenter-Umgebung, die Erfolgsrate des Backups und einige Informationen zu jedem während der festgelegten Zeit durchgeführten Backup. Wenn ein Backup gelöscht wird, zeigt der Bericht keine Statusinformationen für das gelöschte Backup an. Der Bericht Backup Detail enthält detaillierte Informationen zu einem bestimmten Backup-Job und listet die erfolgreich gesicherten Ressourcen und die fehlgeschlagenen Ressourcen auf.
Bericht Klonen	Der Klonbericht enthält allgemeine Daten zu Klon-Trends für Ihre SnapCenter Umgebung, die Erfolgsrate von Klonen und einige Informationen zu jedem Klonjob, der während des festgelegten Zeits ausgeführt wurde. Wenn ein Klon gelöscht wird, zeigt der Bericht keine Statusinformationen für den gelöschten Klon an. Der Detailbericht zum Klonen enthält Details zum angegebenen Klon-, Klon-Host- und Klon-Auftragsstatus. Wenn eine Aufgabe fehlschlägt, zeigt der Detailbericht zum Klonen Informationen über den Fehler an.
Bericht Wiederherstellen	Der Wiederherstellungsbericht enthält allgemeine Informationen zu Wiederherstellungsjobs. Der Detailbericht zur Wiederherstellung enthält Details zu einem festgelegten Wiederherstellungsauftrag, einschließlich Host-Name, Backup-Name, Jobstart und -Dauer sowie Status einzelner Job-Aufgaben. Wenn eine Aufgabe fehlschlägt, zeigt der Detailbericht zur Wiederherstellung Informationen zum Fehler an.
Sicherungsbericht	Diese Berichte enthalten Einzelheiten zu Sicherungsmaßnahmen für Ressourcen, die von allen SnapCenter Plug-in-Instanzen gemanagt werden. Dieser Bericht enthält Sicherungsdetails für Ressourcen, die von allen Plug-in-Instanzen gemanagt werden. Sie sehen eine Übersicht, Details zu ungeschützten Ressourcen, Ressourcen, die zum Zeitpunkt der Berichterstellung nicht gesichert wurden, Ressourcen einer Ressourcengruppe, für die Backup-Vorgänge ausgefallen sind, und den SnapVault-Status.

Berichtstyp	Beschreibung
Planter Bericht	Diese Berichte werden regelmäßig wie täglich, wöchentlich oder monatlich erstellt. Die Berichte werden automatisch zu dem angegebenen Datum und Uhrzeit erstellt und der Bericht wird per E-Mail an die jeweiligen Personen gesendet Sie können die Zeitpläne aktivieren, deaktivieren, ändern oder löschen. Der aktivierte Zeitplan kann auf Anforderung ausgeführt werden, indem Sie auf die Schaltfläche **Jetzt ausführen** klicken. Der Administrator kann einen beliebigen Zeitplan ausführen, der erstellte Bericht enthält jedoch Daten, die auf der Berechtigung des Benutzers basieren, der den Zeitplan erstellt hat. Andere Benutzer als Administrator können den Zeitplan anhand ihrer Berechtigung anzeigen oder ändern. Wenn alle Mitglieder dieser Rolle die Option Objekte anderer Mitglieder auf der Seite Rolle hinzufügen ausgewählt haben, können andere Mitglieder der Rolle sehen und ändern.

Aufrufen von Berichten

Mit dem SnapCenter-Dashboard erhalten Sie einen schnellen Überblick über den Zustand Ihres Systems. Über das Dashboard können Sie weitere Details abrufen. Alternativ können Sie direkt auf detaillierte Berichte zugreifen.

Sie können auf Berichte über eine der folgenden Methoden zugreifen:

- Klicken Sie im linken Navigationsbereich auf **Dashboard** und dann auf **Letzte Schutzübersicht** Kreisdiagramm, um weitere Details auf der Seite Berichte anzuzeigen.
- Klicken Sie im linken Navigationsbereich auf **Berichte**.

Filtern Sie Ihren Bericht

Sie können Ihre Berichtsdaten nach verschiedenen Parametern filtern, je nachdem, wie viel Details und Zeit Sie benötigen.

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 Zeitbereich an, für den der Bericht ausgeführt werden soll. + Wenn Sie das Enddatum nicht angeben, werden alle verfügbaren Informationen abgerufen.
4. Filtern Sie Ihre Berichtsinformationen nach den folgenden Kriterien:
    - Ressourcengruppe
    - Host

- Richtlinie
- Ressource
- Status
- Plug-in-Name

5. Klicken Sie Auf **Anwenden**.

Berichte exportieren oder drucken

Durch das Exportieren von SnapCenter-Berichten können Sie den Bericht in verschiedenen anderen Formaten anzeigen. Sie können auch Berichte drucken.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte**.
2. Führen Sie in der Symbolleiste Berichte 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 **Exportieren**-Symbol 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 Berichtsübersicht anzuzeigen, blättern Sie zum entsprechenden Abschnitt des Berichts.

Stellen Sie den SMTP-Server für E-Mail-Benachrichtigungen ein

Sie können den SMTP-Server angeben, der zum Senden von Datenschutzjobberichten an sich selbst oder 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 die E-Mail-Benachrichtigung konfigurieren.

Mit dieser Option wird der SMTP-Server zum Senden aller Datensicherheitsjobberichte konfiguriert. Wenn Sie jedoch regelmäßige Aktualisierungen für den SnapCenter-Datenschutz für eine bestimmte Ressource an sich selbst oder andere gesendet haben möchten, damit Sie den Status dieser Updates überwachen können, können Sie die Option konfigurieren, die SnapCenter-Berichte per E-Mail zu versenden, wenn Sie eine Ressourcengruppe erstellen.

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 aus Sie die E-Mail senden, geben Sie den Betreff ein und klicken Sie auf **Senden**.

Konfigurieren Sie die Option zum E-Mail-Versenden von Berichten

Wenn Sie regelmäßige Aktualisierungen für den SnapCenter-Datenschutz an sich selbst oder andere Benutzer senden möchten, damit Sie den Status dieser Updates überwachen können, können Sie die Option

konfigurieren, die SnapCenter-Berichte per E-Mail zu senden, wenn Sie eine Ressourcengruppe erstellen.

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 Bereich Benachrichtigung des Assistenten für neue Ressourcengruppe aus dem Pulldown-Menü aus, ob Sie Berichte immer, bei Ausfall, bei Ausfall oder bei Fehler oder Warnung empfangen 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-Repositorys

Informationen zu verschiedenen von SnapCenter durchgeführten Vorgängen werden im Datenbank-Repository des SnapCenter Servers gespeichert. Sie müssen Backups des Repositorys erstellen, um den SnapCenter-Server vor Datenverlust zu schützen.

Das SnapCenter-Server-Repository wird manchmal als NSM-Datenbank bezeichnet.

Voraussetzungen für den Schutz des SnapCenter-Repositorys

Ihre Umgebung sollte bestimmte Voraussetzungen zum Schutz des SnapCenter-Repositorys erfüllen.

- Managen von Storage Virtual Machine-Verbindungen (SVM

  Sie sollten die Speicher-Anmeldeinformationen konfigurieren.

- Bereitstellung von Hosts

  Auf dem SnapCenter Repository-Host sollte mindestens eine NetApp Speicherplatte vorhanden sein. Wenn auf dem SnapCenter Repository-Host kein NetApp-Laufwerk vorhanden ist, müssen Sie ein Laufwerk erstellen.

  Informationen zum Hinzufügen von Hosts, zum Einrichten von SVM-Verbindungen und zum Bereitstellen von Hosts finden Sie in den Installationsanweisungen.

- Bereitstellung von iSCSI LUN oder VMDK

  Für Hochverfügbarkeitskonfigurationen (HA) können Sie ein iSCSI-LUN oder eine VMDK auf einem der SnapCenter-Server bereitstellen.

Sichern des SnapCenter Repositorys

Wenn Sie ein Backup des SnapCenter Server Repositorys durchführen, können Sie diese vor Datenverlust

schützen. Sie können das Repository durch Ausführen des Cmdlet *Protect-SmRepository* sichern.

Über diese Aufgabe

Das Cmdlet *Protect-SmRepository* führt die folgenden Aufgaben aus:

- Erstellt eine Ressourcengruppe und eine Richtlinie
- Erstellt einen Backup-Zeitplan für das SnapCenter-Repository

Schritte

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, 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-Backups von SnapCenter Server anzeigen, indem Sie das Cmdlet *get-SmRepositoryBackups* ausführen.

Die Repository-Backups 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 Anmeldeinformationen für die Verbindung zum SnapCenter-Server an: *Open-SMConnection*
3. Listen Sie alle verfügbaren SnapCenter-Datenbank-Backups mit dem Cmdlet *get-SmoryBackups* auf.

Wiederherstellung des SnapCenter Datenbank-Repositorys

Sie können das SnapCenter-Repository wiederherstellen, indem Sie das Cmdlet *Restore-SmoryBackup* ausführen.

Wenn Sie das SnapCenter-Repository wiederherstellen, sind andere ausgeführte SnapCenter-Vorgänge betroffen, da während des Wiederherstellungsvorgangs die Repository-Datenbank nicht zugänglich ist.

Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung das folgende Cmdlet ein und geben Sie dann Anmeldeinformationen für die Verbindung zum SnapCenter-Server an: *Open-SMConnection*
3. Stellen Sie das Repository-Backup mit dem Cmdlet *Restore-SmRepositoryBackup* wieder her.

   Mit dem folgenden Cmdlet wird das SnapCenter MySQL Datenbank-Repository aus den auf iSCSI LUN oder VMDK vorhandenen Backups wiederhergestellt:

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
   x3550-s09_09-15-2016_10.32.00.4445
   ```

Mit dem folgenden Cmdlet wird die SnapCenter MySQL Datenbank wiederhergestellt, wenn Backup-Dateien versehentlich in der iSCSI-LUN gelöscht werden. Für VMDK stellen Sie 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
```

Das Backup, das zur Durchführung des Repository-Wiederherstellungsvorgangs verwendet wurde, wird nicht aufgeführt, wenn die Repository-Backups nach Durchführung der Wiederherstellung abgerufen werden.

SnapCenter-Repository migrieren

Sie können das Datenbank-Repository des SnapCenter-Servers vom Standardspeicherort auf ein anderes Laufwerk migrieren. Sie können das Repository migrieren, wenn Sie es auf eine Festplatte mit mehr Speicherplatz verschieben möchten.

Schritte

1. Beenden Sie den MYSQL57-Dienst in Windows.
2. Suchen Sie das MySQL-Datenverzeichnis.

   Das Datenverzeichnis finden Sie in der Regel unter C:\ProgramData\MySQL\MySQL Server 5.7\Data.
3. Kopieren Sie das MySQL-Datenverzeichnis in den neuen Speicherort, z. B. E:\Data\nsm.
4. Klicken Sie mit der rechten Maustaste auf das neue Verzeichnis, und wählen Sie dann **Eigenschaften** > **Sicherheit** aus, um das lokale Network Service Server-Konto dem neuen Verzeichnis hinzuzufügen, und weisen Sie dann die volle Kontrolle zu.
5. Benennen Sie das ursprüngliche Datenbankverzeichnis um, z. B. nsm_copy.
6. Erstellen Sie in einer Windows-Eingabeaufforderung mithilfe des Befehls *mklink* einen symbolischen Verzeichnislink.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```
7. Starten Sie den MYSQL57-Dienst unter Windows.
8. Stellen Sie sicher, dass die Änderung des Datenbankstandorts erfolgreich ist, indem Sie sich bei SnapCenter anmelden und 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 (nsm_copy).

Setzen Sie das SnapCenter Repository-Kennwort zurück

Das MySQL Server Repository-Datenbankkennwort wird bei der Installation des SnapCenter Servers von SnapCenter 4.2 automatisch generiert. Dieses automatisch generierte Passwort ist dem SnapCenter-Benutzer an keinem Punkt bekannt. Wenn Sie auf die Repository-Datenbank zugreifen möchten, sollten Sie das Passwort zurücksetzen.

Bevor Sie beginnen

Sie sollten über die SnapCenter-Administratorrechte 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 zum SnapCenter-Server an: *Open-SMConnection*
3. Setzen Sie das Repository-Passwort zurück: *Set-SmRepositoryPassword*

   Mit dem folgenden Befehl wird das Repository-Passwort zurückgesetzt:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

Verwandte Informationen

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Management von Ressourcen von nicht vertrauenswürdigen Domänen

Neben dem Management von Hosts in vertrauenswürdigen Active Directory (AD) Domänen managt SnapCenter auch Hosts in mehreren AD-Domänen, die nicht vertrauenswürdig sind. Die nicht vertrauenswürdigen AD-Domänen müssen beim SnapCenter-Server registriert werden. SnapCenter unterstützt Benutzer und Gruppen aus mehreren nicht vertrauenswürdigen 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, müssen Sie die Domänenanmeldeinformationen angeben, wenn sich der Computer in einer Domäne befindet oder sich die lokalen Administratoranmeldeinformationen befinden, wenn sich der Computer in einer Arbeitsgruppe befindet.

Active Directory-Gruppen (AD), die zu Domänen gehören, die nicht mit dem SnapCenter-Server registriert sind, werden nicht unterstützt. Obwohl Sie SnapCenter-Rollen mit diesen AD-Gruppen erstellen können, schlägt die Anmeldung beim SnapCenter-Server mit der folgenden Fehlermeldung fehl: Der Benutzer, den Sie sich anmelden möchten, gehört nicht zu Rollen. Bitte wenden Sie sich an den Administrator.

Ändern Sie nicht vertrauenswürdige Domains

Sie können eine nicht vertrauenswürdige Domäne ändern, wenn Sie die IP-Adressen des Domänencontrollers oder den vollständig qualifizierten Domänennamen (FQDN) aktualisieren möchten.

Über diese Aufgabe

Nachdem Sie den FQDN geändert haben, funktionieren die zugeordneten Assets (Hosts, Benutzer und Gruppen) möglicherweise nicht wie erwartet.

Zum Ändern einer nicht vertrauenswürdigen Domäne können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell Commandlets 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. Klicken Sie auf  , und geben Sie dann die folgenden Details an:

Für dieses Feld…	Tun Sie das…
Domain-FQDN	Geben Sie den FQDN an, und klicken Sie auf **Auflösen**.
IP-Adressen des Domänencontrollers	Wenn der Domain-FQDN nicht lösbar ist, geben Sie eine oder mehrere IP-Adressen des Domänencontrollers an.

5. Klicken Sie auf **OK**.

Nicht vertrauenswürdige Active Directory-Domänen werden nicht registriert

Sie können die Registrierung einer nicht vertrauenswürdigen Active Directory-Domäne aufheben, wenn Sie die Assets, die dieser Domäne zugeordnet sind, nicht verwenden möchten.

Bevor Sie beginnen

Sie sollten die Hosts, Benutzer, Gruppen und Anmeldeinformationen entfernt haben, die der nicht vertrauenswürdigen Domäne zugeordnet sind.

Über diese Aufgabe

- Nachdem die Domäne vom SnapCenter-Server nicht registriert wurde, können Benutzer dieser Domäne nicht auf den SnapCenter-Server zugreifen.
- Wenn es zugeordnete Assets (Hosts, Benutzer und Gruppen) gibt, sind die Assets nach der Registrierung der Domäne nicht mehr betriebsbereit.
- Um die Registrierung einer nicht vertrauenswürdigen Domäne zu aufheben, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell Commandlets 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 Liste der Domänen die Domain aus, die Sie aufheben möchten.

5. Klicken Sie auf , und klicken Sie dann auf **OK**.

Management des Storage-Systems

Nach dem Hinzufügen des Speichersystems können Sie die Konfiguration und Verbindungen des Speichersystems ändern oder das Speichersystem löschen.

Konfiguration des Storage-Systems ändern

Sie können mit SnapCenter die Konfiguration Ihres Storage-Systems ändern, wenn Sie den Benutzernamen, das Passwort, die Plattform, Port, das Protokoll, ändern möchten. Timeout-Zeitraum, bevorzugte IP-Adresse oder Messaging-Optionen.

Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe ändern. Wenn Sie einer oder mehreren Gruppen mit Berechtigung zum selben Speichersystem angehören, wird der Name der Speicherverbindung mehrfach in der Liste der Speicherverbindungen 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 Storage Systems aus dem Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

Auswählen…	Schritte…
ONTAP SVMs	So können alle hinzugefügten Storage Virtual Machines (SVMs) und die erforderliche SVM-Konfiguration angezeigt werden. a. Klicken Sie auf der Seite Storage Connections auf den entsprechenden SVM-Namen. b. Führen Sie eine der folgenden Aktionen aus: ◦ Wenn die SVM nicht Teil eines Clusters ist, ändern Sie auf der Seite „Speichersystem ändern“ die Konfigurationen wie Benutzername, Passwort, EMS- und AutoSupport-Einstellungen, Plattform, Protokoll, Port, Timeout Und bevorzugte IP-Adresse. ◦ Wenn die SVM Teil eines Clusters ist, wählen Sie auf der Seite Speichersystem ändern die Option **SVM unabhängig managen** aus und ändern Sie die Konfigurationen wie Benutzername, Passwort, EMS- und AutoSupport-Einstellungen, Plattform, Protokoll, Port, Timeout, Und bevorzugte IP-Adresse. Nachdem Sie die SVM für das unabhängige Management geändert haben und sich für das Management über den Cluster entscheiden, sollten Sie die SVM löschen und dann auf **neu entdeckt** klicken. Die SVM wird dem ONTAP-Cluster hinzugefügt. Wenn ein Speichersystemkennwort auf der SnapCenter-GUI aktualisiert wird, sollten Sie die SMCore-Dienste des jeweiligen Plug-ins oder des Server-Hosts neu starten, da das aktualisierte Passwort nicht in SMCore reflektiert wird, und die Backupjobs mit einem falschen Anmeldeinformationsfehler fehlschlagen.

Auswählen…	Schritte…
ONTAP Cluster	Anzeige aller hinzugefügten Cluster und Änderung der erforderlichen Cluster-Konfiguration a. Klicken Sie auf der Seite Storage Connections auf den Cluster-Namen. b. Klicken Sie auf der Seite Speichersystem ändern auf das Bearbeiten-Symbol neben Benutzername und ändern Sie den Benutzernamen und das Kennwort. c. Wählen Sie die EMS- und AutoSupport-Einstellungen aus oder löschen Sie diese. d. Klicken Sie auf **Weitere Optionen** und ändern Sie andere Konfigurationen wie Plattform, Protokoll, Port, Timeout und bevorzugte IP.

3. Klicken Sie Auf **Absenden**.

Löschen Sie das Speichersystem

Sie können SnapCenter verwenden, um alle nicht verwendeten Speichersysteme zu löschen.

Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe löschen. Wenn Sie einer oder mehreren Gruppen mit Berechtigung zum selben Speichersystem angehören, wird der Name des Speichersystems mehrfach in der Liste der Speicherverbindungen angezeigt, einmal für jede Gruppe mit Berechtigung für das Speichersystem.

Wenn Sie ein Storage-System löschen, fallen alle Vorgänge aus, die auf diesem Storage-System ausgeführt werden, aus.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Wählen Sie auf der Seite Speichersysteme im Dropdown-Menü **Typ** entweder **ONTAP-SVMs** oder **ONTAP-Cluster** aus.
3. Aktivieren Sie auf der Seite Storage Connections das Kontrollkästchen neben der SVM oder das Cluster, das Sie löschen möchten.

   Sie können keine SVM auswählen, die Teil eines Clusters ist.

4. Klicken Sie Auf **Löschen**.
5. Klicken Sie auf der Seite Einstellungen für die Speichersystemverbindung löschen auf **OK**.

   Wenn eine SVM aus dem ONTAP-Cluster mithilfe der ONTAP-GUI gelöscht wird, klicken Sie in der SnapCenter-GUI auf **erneut entdecken**, um die SVM-Liste zu aktualisieren.

EMS-Datenerfassung managen

Sie können die Datenerfassung im Event Management System (EMS) mithilfe von PowerShell Cmdlets planen und verwalten. Die EMS-Datenerfassung umfasst die Sammlung von Details zum SnapCenter-Server, den installierten SnapCenter-Plug-in-Paketen, den Hosts und ähnlichen Informationen und sendet sie dann an eine bestimmte ONTAP Storage Virtual Machine (SVM).

Die CPU-Auslastung des Systems ist hoch, wenn gerade die Datenerfassung läuft. Die CPU-Auslastung bleibt hoch, solange der Betrieb unabhängig von der Datengröße fortschreitet.

EMS-Datenerfassung stoppen

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird alle sieben Tage nach dem Installationsdatum ausgeführt. Sie können die Datenerfassung jederzeit mit dem PowerShell Cmdlet *Disable-SmDataCollectionEMS* deaktivieren.

Schritte

1. Erstellen Sie in einer PowerShell-Befehlszeile eine Sitzung mit SnapCenter, indem Sie *Open-SmConnection* eingeben.
2. Deaktivieren Sie die EMS-Datensammlung, indem Sie *Disable-SmDataCollectionEms* eingeben.

Starten Sie die EMS-Datensammlung

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird voraussichtlich alle sieben Tage ab dem Installationsdatum ausgeführt. Wenn Sie die EMS-Datensammlung deaktiviert haben, können Sie die EMS-Datensammlung erneut mit dem Cmdlet *enable-SmDataCollectionEMS* starten.

Die Berechtigung zum Generieren des Data ONTAP-Events „Generate-AutoSupport-log“ wurde dem SVM-Benutzer (Storage Virtual Machine) zugewiesen.

Schritte

1. Erstellen Sie in einer PowerShell-Befehlszeile eine Sitzung mit SnapCenter, indem Sie *Open-SmConnection* eingeben.
2. Aktivieren Sie die EMS-Datensammlung, indem Sie *enable-SmDataCollectionEMS* eingeben.

EMS-Datenerfassungsplan und Ziel-SVM ändern

Mit PowerShell cmdlets können Sie den EMS-Zeitplan zur Datenerfassung oder die Ziel-Storage Virtual Machine (SVM) ändern.

Schritte

1. Geben Sie in einer PowerShell-Befehlszeile zum Erstellen einer Sitzung mit SnapCenter das Cmdlet *Open-SmConnection* ein.
2. Um das EMS-Datenerfassungsziel zu ändern, geben Sie das Cmdlet *set-SmDataCollectionEmsTarget* ein.
3. Um den EMS-Datenerfassungsplan zu ändern, geben Sie das Cmdlet *set-SmDataCollectionEmsSchedule* ein.

Den EMS-Datenerfassungsstatus überwachen

Sie können den Status Ihrer EMS-Datensammlung mithilfe mehrerer PowerShell Commandlets überwachen. Sie erhalten Informationen zum Zeitplan, zum Storage Virtual Machine-Ziel (SVM) und zum Status.

Schritte

1. Erstellen Sie in einer PowerShell-Befehlszeile eine Sitzung mit SnapCenter, indem Sie *Open-SmConnection* eingeben.
2. Rufen Sie Informationen zum EMS-Datenerfassungsplan ab, indem Sie *get-SmDataCollectionEmsSchedule* eingeben.
3. Rufen Sie Informationen zum EMS-Datenerfassungsstatus ab, indem Sie *get-SmDataCollectionEmsStatus* eingeben.
4. Rufen Sie Informationen zum EMS-Datenerfassungsziel ab, indem Sie *get-SmDataCollectionEmsTarget* eingeben.

Verwandte Informationen

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Aktualisieren Sie SnapCenter Server und Plug-ins

Konfigurieren Sie SnapCenter, um nach verfügbaren Updates zu suchen

SnapCenter kommuniziert regelmäßig mit der NetApp Support-Website, um Sie über verfügbare Software Updates zu informieren. Sie können auch einen Zeitplan erstellen, in dem das Intervall angegeben wird, in dem Informationen über verfügbare Updates empfangen werden sollen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf **Software**.

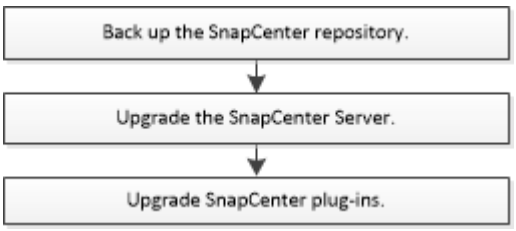
   Auf der Seite Verfügbare Software werden die verfügbaren Plug-in-Pakete, verfügbaren Versionen und deren Installationsstatus angezeigt.

3. Klicken Sie auf **nach Updates suchen**, um zu sehen, ob neuere Versionen von Plug-in-Paketen zur Verfügung stehen.
4. Klicken Sie auf **Updates planen**, um einen Zeitplan zu erstellen, in dem das Intervall angegeben wird, in dem Sie Informationen über verfügbare Aktualisierungen erhalten möchten:
   a. Wählen Sie das Intervall in **nach Updates suchen** aus.
   b. Wählen Sie die Windows-Anmeldedaten für SnapCenter Server Admin aus, und klicken Sie auf **OK**.

Workflow-Upgrade

Jede Version von SnapCenter enthält einen aktualisierten SnapCenter-Server und ein Plug-in-Paket. Plug-in-Paketaktualisierungen werden mit dem SnapCenter-Installationsprogramm verteilt. Sie können SnapCenter konfigurieren, um nach verfügbaren Updates zu suchen.

Der Workflow zeigt die verschiedenen Aufgaben, die zum Upgrade des SnapCenter-Servers und der Plug-in-Pakete erforderlich sind.



Unterstützte Upgrade-Pfade

Wenn Sie sich auf SnapCenter Server-Version befinden…	Sie können ein Upgrade des SnapCenter-Servers direkt auf…	Unterstützte Plug-in-Versionen
4,9	5,0	• 4,9 • 5,0
	6,0	• 6,0
5,0	6,0	• 5,0 • 6,0
	6.0.1	• 6.0.1
6,0	6.0.1	• 6,0 • 6.0.1

Wenn Sie beispielsweise SnapCenter Version 4.9 verwenden und auf 6.0 aktualisieren möchten, sollten Sie zuerst ein Upgrade auf 5.0 durchführen und dann ein Rolling Upgrade auf 6.0 durchführen.

Informationen zum Upgrade des SnapCenter-Plug-ins für VMware vSphere finden Sie unter "Aktualisieren Sie das SnapCenter Plug-in für 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

- Der SnapCenter-Server-Host muss mit Windows-Updates auf dem neuesten Stand sein, ohne dass das System neu gestartet werden muss.
- Stellen Sie sicher, dass keine anderen Vorgänge ausgeführt werden, bevor Sie mit dem Upgrade beginnen.
- 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 des SnapCenter Repositorys".

- Sichern Sie alle geänderten SnapCenter -Konfigurationsdateien entweder auf dem SnapCenter Server-Host oder dem Plug-In-Host.

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" .

Über diese Aufgabe

- 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 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, für DIE Ausführung VON SCRIPTS_PATH sowohl den Server als auch die Plug-in-Hosts auf die Version 4.7 zu aktualisieren.

  Für die bestehenden Backup- und Verifizierungspläne mit aktivierten in der Richtlinie aktivierten Prescripts und Postscripts funktionieren die Backup-Vorgänge nach dem Upgrade weiterhin.

  Auf der Seite **Job Details** empfiehlt eine Warnmeldung, dass der Kunde die Skripte in DEN SCRIPTS_PATH kopieren und die Richtlinie bearbeiten sollte, um einen Pfad bereitzustellen, der sich auf den SCRIPTS_PATH bezogen. Für den Clone Lifecycle Job wird die Warnmeldung auf der Unterauftragsebene angezeigt.

Schritte

1. Laden Sie das SnapCenter Server-Installationspaket von der NetApp Support Website herunter.

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. Erstellen Sie eine Kopie von 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 das Repository-Backup 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 Passwort 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. Beheben Sie alle Fehler, bevor Sie fortfahren. Sie können Warnungen ignorieren und fortfahren.

SnapCenter verwendet weiterhin das vorhandene Datenbankkennwort für das MySQL-Server-Repository, das bei der Installation der früheren Version von SnapCenter Server angegeben wurde.

6. Wählen Sie **Upgrade**.

   Wenn Sie zu irgendeinem Zeitpunkt **Abbrechen** auswählen, stoppt SnapCenter das Upgrade. Der SnapCenter -Server wird nicht in seinen vorherigen Zustand zurückgesetzt.

   Best Practice: Melden Sie sich ab und erneut an oder öffnen Sie einen neuen Browser, um auf die SnapCenter Benutzeroberfläche zuzugreifen.

Nachdem Sie fertig sind

- Wenn das Plug-in mit einem Sudo-Benutzer installiert wird, sollten Sie die unter *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_Plugins_Checksumme.txt* verfügbaren sha224-Schlüssel kopieren, um die */etc/sudoers*-Datei zu aktualisieren.
- Sie sollten eine neue Ermittlung der Ressourcen auf dem Server-Host 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 vorherige SnapCenter -Version neu und stellen Sie den vorherigen Zustand der NSM-Datenbank wieder her.
- Nach dem Upgrade des Server-Hosts müssen Sie auch die Plug-ins aktualisieren, bevor Sie ein Speichersystem hinzufügen.

Aktualisieren Sie den SnapCenter-Server auf dem Linux-Host

Sie können die Installationsdatei des SnapCenter-Servers verwenden, um den SnapCenter-Server zu aktualisieren.

Schritte

1. Führen Sie eine der Aktionen zum Aktualisieren des SnapCenter-Servers durch.

Wenn Sie Folgendes ausführen möchten:	Tun Sie das…
Nicht-interaktives Upgrade	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename>` Beispiel: Sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log Protokolle werden unter */var/opt/snapcenter/logs* gespeichert. Parameter, die für die Aktualisierung übergeben werden müssen: • DINSTALL_LOG_NAME: NAME der Protokolldatei, in der die Installationsprotokolle gespeichert werden. • DUPGRADE: Der Standardwert ist 0. Geben Sie diesen Parameter und seinen Wert als eine ganze Zahl außer 0 an, um den SnapCenter-Server zu aktualisieren.
Interaktive Installation	`./snapcenter-linux-server-(el8/el9/sles15).bin` Sie werden aufgefordert, das Upgrade zu bestätigen. Geben Sie einen anderen Wert als 0 ein, um das Upgrade des SnapCenter-Servers zu bestätigen.

Sie sollten sich entweder aus- und anschließend bei SnapCenter anmelden oder schließen und dann einen neuen Browser öffnen, um auf die SnapCenter GUI zuzugreifen.

Aktualisieren Sie Ihre Plug-in-Pakete

Die Plug-in-Pakete werden im Rahmen des SnapCenter Upgrades verteilt.

Sie müssen nicht jeden Plug-in-Host, den Sie aktualisieren möchten, manuell in den Wartungsmodus versetzen, da das Upgrade 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 nicht-Root-Benutzer mit Zugriff auf die Linux-Maschinen sind, sollten Sie die Datei */etc/sudoers* vor der Durchführung des Upgrade-Vorgangs mit den neuesten Prüfsummenwerten aktualisieren.
- Standardmäßig erkennt SnapCenter JAVA_HOME von der Umgebung. Wenn Sie eine feste JAVA_HOME-DATEI verwenden möchten und wenn Sie die Plug-ins auf einem Linux-Host aktualisieren, sollten Sie den

PARAMETER SKIP_JAVAHOME_UPDATE manuell in die 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 SPL-Dienst (Plug-in Loader) von SnapCenter neu startet. Wenn Sie vor dem Aktualisieren 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 sichern, 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.

Über diese Aufgabe

- 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 für DIE Ausführung VON SCRIPTS_PATH zu aktualisieren.

  Für die bestehenden Backup- und Verifizierungspläne mit aktivierten in der Richtlinie aktivierten Prescripts und Postscripts funktionieren die Backup-Vorgänge nach dem Upgrade weiterhin.

  Auf der Seite **Job Details** empfiehlt eine Warnmeldung, dass der Kunde die Skripte in DEN SCRIPTS_PATH kopieren und die Richtlinie bearbeiten sollte, um einen Pfad bereitzustellen, der sich auf den SCRIPTS_PATH bezogen. Für den Clone Lifecycle Job wird die Warnmeldung auf der Unterauftragsebene 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-inhosts „Upgrade verfügbar“ angezeigt wird, klicken Sie auf den Plug-in-Hostnamen, und führen Sie die folgenden Schritte aus:

     i. Klicken Sie Auf **Weitere Optionen**.

     ii. Wählen Sie **Vorabprüfungen überspringen** aus, wenn Sie nicht überprüfen möchten, ob der Plug-in-Host die Anforderungen für ein Upgrade des Plug-ins erfüllt.

     iii. Klicken Sie Auf **Upgrade**.

   - Wenn Sie mehrere Plug-in-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 SnapCenter-Version installiert wurden, werden aktualisiert, und die übrigen Plug-ins sind nicht installiert. Sie müssen die Option **Add Plug-ins** verwenden, um ein neues Plug-in zu installieren.

     Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird der Plug-in-Host überprüft, ob er die Anforderungen für die Installation des Plug-ins erfüllt. Wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen

angezeigt. Klicken Sie nach Behebung des Problems auf **Upgrade**.

Wenn der Fehler mit dem Festplattenspeicher 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 den übrigen Parametern zusammenhängt, müssen Sie das Problem beheben und anschließend die Anforderungen erneut überprüfen.

Technologieaktualisierung

Technologieaktualisierung des SnapCenter-Serverhosts

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 die 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 "Konfigurieren Sie das CA-Zertifikat" und "Konfigurieren und aktivieren Sie bidirektionale SSL-Verbindungen".
   c. (Optional) Konfigurieren Sie die Multi-Faktor-Authentifizierung. Weitere Informationen finden Sie unter "Multi-Faktor-Authentifizierung aktivieren".
2. Melden Sie sich als SnapCenter-Admin-Benutzer an.
3. Erstellen Sie eine Sicherung des SnapCenter-Servers auf dem alten Host entweder mit der API: Oder mit `/<snapcenter_version>/server/backup` dem Cmdlet: *New-SmServerBackup*.

   Bevor Sie die Sicherung durchführen, halten Sie alle geplanten Jobs an, und stellen Sie sicher, dass keine Jobs ausgeführt werden.

   Wenn Sie das Backup auf dem SnapCenter-Server wiederherstellen möchten, der auf einer neuen Domäne ausgeführt wird, müssen Sie vor dem Erstellen eines Backups den neuen Domänenbenutzer dem alten SnapCenter-Host hinzufügen und 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 entweder mit der API: Oder mit dem Cmdlet: *Restore-SmServerBackup* wieder `/<snapcenter_version>/server/restore` her.

   Die Wiederherstellung aktualisiert standardmäßig die neue SnapCenter-Server-URL in allen Hosts. Wenn Sie das Update überspringen möchten, verwenden Sie das *-SkipSMSURLInHosts*-Attribut und aktualisieren Sie die Server-URL separat, indem Sie entweder die API: Oder das Cmdlet: *Set-SmServerConfig* ausführen `/<snapcenter_version>/server/configureurl` .

   Wenn der Plug-in-Host den Server-Hostnamen nicht auflösen kann, melden Sie sich bei jedem Plug-in-Host an und fügen Sie den „*etc/Host*“-Eintrag für die neue IP im Format „<New IP> SC_Server_Name“ hinzu.

   Die Einträge des Servers *etc/Host* werden nicht wiederhergestellt. Sie können es manuell vom alten Server wiederherstellen.

   Wenn das Backup auf dem SnpCenter-Server wiederhergestellt wird, der auf einer neuen Domäne ausgeführt wird, und wenn Sie weiterhin die alten Domänenbenutzer 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 die gleichen 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 Wiederherstellungsprozesses ausgefallen war, aktualisieren Sie den neuen Servernamen in allen Hosts oder angegebenen Hosts, die vom SnapCenter entweder über die API: Oder das Cmdlet: *Set-SmServerConfig* verwaltet `/<snapcenter_version>/server/configureurl` werden.
7. Aktivieren Sie die geplanten Jobs auf allen Hosts vom neuen SnapCenter-Server aus.

Tech Refresh eines Node in F5 Cluster

Sie können jeden beliebigen Knoten im F5-Cluster durch Entfernen des Knotens und Hinzufügen des neuen Knotens aktualisieren. Wenn der Node, der aktualisiert werden muss, aktiv ist, machen Sie einen anderen Node des Clusters als aktiv, und entfernen Sie dann den Node.

Informationen zum Hinzufügen eines Knotens zum F5-Cluster finden Sie unter "Konfiguration von SnapCenter-Servern für Hochverfügbarkeit mit F5".

> Wenn sich die url des F5-Clusters ändert, kann die url auf allen Hosts entweder über die API: Oder über das Cmdlet: *Set-SmServerConfig* aktualisiert werden `/<snapcenter_version>/server/configureurl` .

Den alten SnapCenter-Server-Host stilllegen

Sie können den alten SnapCenter-Server-Host entfernen, nachdem Sie überprüft haben, ob der neue SnapCenter-Server betriebsbereit ist und alle Plug-in-Hosts mit dem neuen SnapCenter-Server kommunizieren können.

Rollback auf den alten SnapCenter-Server-Host durchführen

Im Falle von Problemen können Sie den alten SnapCenter-Server-Host zurückbringen, indem Sie die SnapCenter-Server-URL in allen Hosts entweder über die API: Oder das Cmdlet: *Set-SmServerConfig* aktualisieren `/<snapcenter_version>/server/configureurl` .

Disaster Recovery

Disaster Recovery von Standalone-SnapCenter-Host

Sie können eine Disaster Recovery durchführen, indem Sie die Serversicherung auf dem neuen Host wiederherstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über ein Backup 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 von CA-Zertifikaten und Aktivieren von bidirektionalem SSL. Weitere Informationen finden Sie unter "Konfigurieren Sie das CA-Zertifikat" und "Konfigurieren und aktivieren Sie bidirektionale SSL-Verbindungen".

2. Kopieren Sie das alte SnapCenter-Server-Backup auf den neuen Host.
3. Melden Sie sich als SnapCenter-Admin-Benutzer an.
4. Stellen Sie die Sicherung des SnapCenter-Servers auf dem neuen Host entweder mit der API: Oder mit dem Cmdlet: *Restore-SmServerBackup* wieder `/<snapcenter_version>/server/restore` her.

   Die Wiederherstellung aktualisiert standardmäßig die neue SnapCenter-Server-URL in allen Hosts. Wenn Sie das Update überspringen möchten, verwenden Sie das *-SkipSMSURLInHosts*-Attribut und aktualisieren Sie die Server-URL separat, indem Sie entweder die API: `/<snapcenter_version>/server/configureurl` Oder das Cmdlet: *Set-SmServerConfig* verwenden.

   Wenn der Plug-in-Host den Server-Hostnamen nicht auflösen kann, melden Sie sich bei jedem Plug-in-Host an und fügen Sie den „*etc/Host*“-Eintrag für die neue IP im Format „<New IP> SC_Server_Name“ hinzu.

   Die Einträge des Servers *etc/Host* 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 Wiederherstellungsprozesses ausgefallen war, aktualisieren Sie den neuen Servernamen in allen Hosts oder angegebenen Hosts, die vom SnapCenter entweder über die API: Oder das Cmdlet: *Set-SmServerConfig* verwaltet werden `/<snapcenter_version>/server/configureurl` .

Disaster Recovery von SnapCenter F5 Clustern

Sie können eine Disaster Recovery durchführen, indem Sie das Server-Backup auf dem neuen Host wiederherstellen und dann den eigenständigen Host in einen Cluster konvertieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über ein Backup 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 von CA-Zertifikaten und Aktivieren von bidirektionalem SSL. Weitere Informationen finden Sie unter "Konfigurieren Sie das CA-Zertifikat" und "Konfigurieren und aktivieren Sie bidirektionale SSL-Verbindungen".
2. Kopieren Sie das alte SnapCenter-Server-Backup auf den neuen Host.
3. Melden Sie sich als SnapCenter-Admin-Benutzer an.
4. Stellen Sie die Sicherung des SnapCenter-Servers auf dem neuen Host entweder mit der API: Oder mit dem Cmdlet: *Restore-SmServerBackup* wieder `/<snapcenter_version>/server/restore` her.

   Die Wiederherstellung aktualisiert standardmäßig die neue SnapCenter-Server-URL in allen Hosts. Wenn Sie das Update überspringen möchten, verwenden Sie das *-SkipSMSURLInHosts*-Attribut und aktualisieren Sie die Server-URL separat, indem Sie entweder die API: `/<snapcenter_version>/server/configureurl` Oder das Cmdlet: *Set-SmServerConfig*

verwenden.

Wenn der Plug-in-Host den Server-Hostnamen nicht auflösen kann, melden Sie sich bei jedem Plug-in-Host an und fügen Sie den „*etc/Host*“-Eintrag für die neue IP im Format „<New IP> SC_Server_Name“ hinzu.

Die Einträge des Servers *etc/Host* 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 Wiederherstellungsprozesses ausgefallen war, aktualisieren Sie den neuen Servernamen in allen Hosts oder angegebenen Hosts, die vom SnapCenter entweder über die API: Oder das Cmdlet: *Set-SmServerConfig* verwaltet werden `/<snapcenter_version>/server/configureurl` .
6. Konvertieren Sie den Standalone-Host in F5-Cluster.

   Informationen zum Konfigurieren von F5 finden Sie unter "Konfiguration von SnapCenter-Servern für Hochverfügbarkeit mit F5".

Verwandte Informationen

Für Informationen zu den APIs müssen Sie auf die Seite Swagger zugreifen. "Zugriff auf REST-APIs über die Swagger-API-Webseite"Siehe .

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch die "SnapCenter Software Cmdlet Referenzhandbuch".

Technologieaktualisierung bei SnapCenter Plug-in-Hosts

Wenn die SnapCenter-Plug-in-Hosts aktualisiert werden müssen, sollten Sie die Ressourcen vom alten Host auf einen neuen Host verschieben. Wenn der neue Host zu SnapCenter hinzugefügt wird, erkennt er alle Ressourcen, wird aber als neue Ressourcen behandelt.

Über diese Aufgabe

Sie sollten die API oder das Cmdlet ausführen, die den alten Hostnamen und den neuen Hostnamen als Eingabe übernehmen, die Ressourcen nach Namen vergleichen und die Objekte der übereinstimmenden Ressourcen vom alten Host mit dem neuen Host neu verknüpfen. Die übereinstimmenden Ressourcen werden als geschützt markiert.

- Der Parameter *IsDryRun* ist standardmäßig auf true gesetzt und identifiziert die passenden Ressourcen des alten und des 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 wieder mit dem neuen Host 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* gilt nur für Oracle- und SAP HANA-Ressourcen.

- 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 Instanzname.

Die Technologieaktualisierung wird von den folgenden SnapCenter-Plug-ins unterstützt:

- SnapCenter Plug-in für Microsoft SQL Server
  - Wenn die SQL-Datenbanken auf Instanzebene geschützt sind und im Rahmen der Erneuerung der Host-Technologie nur Teilressourcen auf neuen Host verschoben werden, wird der Schutz auf der vorhandenen Instanzebene in den Schutz der Ressourcengruppen umgewandelt und Instanzen beider Hosts werden der Ressourcengruppe hinzugefügt.
  - Wenn ein SQL-Host (z. B. host1) als Scheduler oder Verifikationsserver für Ressourcen eines anderen Hosts (z. B. host2) verwendet wird, wird der Zeitplan oder die Überprüfungsdetails während der Tech Refresh 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 die Einrichtung von SQL Failover Cluster Instances (FCI) verwenden, können Sie die Technologieaktualisierung durchführen, indem Sie den neuen Knoten zum FCI-Cluster hinzufügen und den Plug-in-Host in SnapCenter aktualisieren.
  - Wenn Sie das Setup der SQL Availability Group (AG) verwenden, ist keine Technologieaktualisierung 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 Database

  Wenn Sie das Oracle RAC-Setup (Real Application Cluster) verwenden, können Sie die Technologieaktualisierung durchführen, indem Sie den neuen Knoten zum RAC-Cluster hinzufügen und den Plug-in-Host in SnapCenter aktualisieren.
- SnapCenter-Plug-in für SAP HANA Database

Folgende Anwendungsfälle werden unterstützt:

- Migration 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

Folgende Szenarien werden unterstützt:

- Neuer 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, ein Backup des SnapCenter-Repository zu erstellen. Falls ein Datenprobleme auftreten, kann das SnapCenter Repository mithilfe des Backups in den alten Status zurückgesetzt werden.

Weitere Informationen finden Sie unter "Sichern des SnapCenter Repositorys".

Schritte

1. Implementieren Sie den neuen Host, und installieren Sie die Anwendung.

2. Unterbrechen Sie die Zeitpläne des alten Hosts.
3. Verschieben Sie die erforderlichen Ressourcen vom alten Host auf den neuen Host.
   a. Erstellen Sie die erforderlichen Datenbanken auf dem neuen Host von demselben Storage.
      - Stellen Sie sicher, dass der Speicher dem gleichen Laufwerk oder dem gleichen Mount-Pfad wie der alte Host zugeordnet ist. Wenn der Speicher nicht korrekt zugeordnet ist, können Backups, die auf dem alten Host erstellt wurden, nicht für die Wiederherstellung verwendet werden.

        Standardmäßig weist Windows das nächste verfügbare Laufwerk automatisch zu.

      - Wenn Storage DR aktiviert ist, sollte der entsprechende Speicher in den neuen Host eingebunden werden.

   b. Prüfen Sie die Kompatibilität, wenn sich die Anwendungsversion geändert hat.
   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 identisch sind.

      Weitere Informationen finden Sie unter:

      - "So migrieren Sie die SQL-Datenbank vom alten Host auf den neuen Host"
      - "So migrieren Sie die Oracle-Datenbank von einem alten Host auf einen neuen Host"
      - "Wie man SAP HANA Datenbank auf neuen Host aufstellt"
4. Fügen Sie den neuen Host zu SnapCenter hinzu.
5. Überprüfen Sie, ob alle Ressourcen erkannt wurden.
6. Führen Sie die Host Refresh API: `/<snapcenter_version>/techrefresh/host` Oder das Cmdlet: *Invoke-SmTechRefreshHost* aus.

   Der Probelauf ist standardmäßig aktiviert, und die entsprechenden Ressourcen werden identifiziert, die neu verknüpft werden sollen. 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 im neuen Host nicht mit dem alten Host identisch ist, schlagen die folgenden Wiederherstellungsvorgänge fehl:

   - Die SQL-Wiederherstellung vor Ort schlägt fehl. Die RTAL-Funktion kann jedoch genutzt werden.
   - Bei der Wiederherstellung von Oracle- und SAP HANA-Datenbanken wird ein Ausfall auftreten.

   Wenn Sie zu mehreren Hosts migrieren möchten, sollten Sie alle Schritte aus Schritt 1 für alle Hosts ausführen.

   Sie können die API oder das Cmdlet mehrmals auf demselben Host ausführen, es wird nur dann erneut verbunden, wenn eine neue Ressource identifiziert wurde.

7. (Optional) Entfernen Sie den alten Host oder die alten Hosts aus SnapCenter.

Verwandte Informationen

Für Informationen zu den APIs, müssen Sie auf die Seite Swagger zugreifen. "Zugriff auf REST-APIs über die Swagger-API-Webseite"Siehe .

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch die "SnapCenter Software Cmdlet Referenzhandbuch".

Technologieaktualisierung des Storage-Systems

Nach der technischen Aktualisierung des Storage werden die Daten auf neuen Storage migriert und die Applikations-Hosts mit neuem Storage gemountet. Der SnapCenter Backup Workflow identifiziert den neuen Storage und erstellt den Snapshot, wenn der neue Storage in SnapCenter registriert wird.

Sie können die neuen Backups wiederherstellen, mounten und klonen, die nach der Speicheraktualisierung erstellt wurden. Diese Vorgänge schlagen jedoch fehl, wenn sie für die Backups durchgeführt werden, die vor der Speicheraktualisierung erstellt wurden, da die Backups die alten Speicherdetails haben. Sie sollten die Storage Tech Refresh API oder das Cmdlet ausführen, um die alten Backups in SnapCenter mit den neuen Speicherdetails zu aktualisieren.

Die Technologieaktualisierung wird von den folgenden SnapCenter-Plug-ins unterstützt:

- SnapCenter Plug-in für Microsoft SQL Server
- SnapCenter Plug-in für Windows
- SnapCenter Plug-in für Oracle Database
- SnapCenter-Plug-in für SAP HANA Database
- SnapCenter Plug-in für Microsoft Exchange Server

Folgende Anwendungsfälle werden unterstützt:

- Aktualisierung des primären Storage

  Die Aktualisierung der Storage-Technologie wird unterstützt, um den primären Storage durch neuen Storage zu ersetzen. Sie können den vorhandenen sekundären Speicher nicht in einen primären Speicher umwandeln.

- Aktualisierung des sekundären Storage

Die anderen unterstützten Szenarien sind:

- Änderung des SVM-Namens
- Änderung des Volume-Namens

Aktualisieren Sie die Backups des primären Speichers

Wenn der Speicher aktualisiert wird, sollten Sie die Storage Tech Refresh API oder das Cmdlet ausführen, um die alten Backups in SnapCenter mit den neuen Speicherdetails zu aktualisieren.

Bevor Sie beginnen

Da dieser Workflow die Daten im SnapCenter Repository ändert, wird empfohlen, ein Backup des SnapCenter-Repository zu erstellen. Falls ein Datenprobleme auftreten, kann das SnapCenter Repository mithilfe des Backups in den alten Status zurückgesetzt werden.

Weitere Informationen finden Sie unter "Sichern des SnapCenter Repositorys".

Schritte

1. Migrieren der Daten von altem Storage zu neuem Storage

   Weitere Informationen zur Migration finden Sie unter:

   - "Daten zu neuem Storage migrieren"
   - "Wie kann ich ein Volume kopieren und alle Snapshot Kopien beibehalten?"
2. Versetzen Sie den Host in den Wartungsmodus.
3. Den neuen Storage in die jeweiligen Hosts mounten und die Datenbanken einrichten.

   Der neue Speicher sollte wie zuvor mit dem Host verbunden werden. Wenn sie beispielsweise als SAN verbunden war, muss sie als SAN verbunden werden.

   Der neue Storage muss auf demselben Laufwerk oder Pfad wie der alte Storage gemountet werden.
4. Vergewissern Sie sich, dass alle Ressourcen betriebsbereit sind.
5. Fügen Sie den neuen Speicher in SnapCenter hinzu.

   Stellen Sie sicher, dass ein eindeutiger SVM-Name über Cluster in SnapCenter hinweg vorhanden ist. Wenn Sie denselben SVM-Namen im neuen Storage verwenden und alle Volumes der SVM vor der Storage-Aktualisierung migriert werden können, anschließend wird empfohlen, die SVM im alten Cluster zu löschen und den alten Cluster in SnapCenter neu zu ermitteln, wodurch die SVM aus dem Cache entfernt wird.
6. Versetzen Sie den Host in den Produktionsmodus.
7. Erstellen Sie in SnapCenter ein Backup der Ressourcen, deren Speicher migriert wird. SnapCenter benötigt ein neues Backup, um den aktuellsten Storage-Platzbedarf zu ermitteln und mithilfe dieses Backups die Metadaten bestehender alter Backups zu aktualisieren.

   > Sobald eine neue LUN mit dem Host verbunden ist, wird sie über eine neue Seriennummer verfügen. Während der Ermittlung des Windows-Dateisystems behandelt SnapCenter jede eindeutige Seriennummer als neue Ressource. Während der Aktualisierung der Storage-Technologie, wenn die LUN aus dem neuen Storage mit dem Host mit demselben Laufwerksbuchstaben oder Pfad verbunden ist, die Ermittlung des Windows-Dateisystems in SnapCenter markiert die vorhandene Ressource als gelöscht, selbst wenn sie mit demselben Laufwerksbuchstaben oder Pfad gemountet ist, und zeigt die neue LUN als neue Ressource an. Wenn die Ressource als gelöscht gekennzeichnet ist, wird sie in SnapCenter nicht für eine Aktualisierung der Storage-Technologie in Betracht gezogen. Außerdem gehen alle Backups der alten Ressource verloren. Wenn immer eine Speicheraktualisierung stattfindet, sollte für Windows-Dateisystemressourcen die Ressourcenerkennung nicht vor der Ausführung der Speicheraktualisierungs-API oder des Cmdlet ausgeführt werden.
8. Führen Sie entweder die Speicher-Refresh-API aus: `/<snapcenter_version>/techrefresh/primarystorage` Oder das Cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   > Wenn die Ressource mit einer Richtlinie für die aktivierte Replikation konfiguriert ist, sollte das letzte Backup nach der Speicheraktualisierung Details zum sekundären Speicher enthalten.

   a. Wenn Sie SQL Failover Cluster Instances (FCI) einrichten, werden die Backups auf Cluster-Ebene

beibehalten. Sie sollten den Cluster-Namen als Eingabe für die Aktualisierung der Storage-Technologie angeben.

b. Wenn Sie SQL Availability Group (AG)-Setup verwenden, werden die Backups auf Node-Ebene beibehalten. Sie sollten den Node-Namen als Eingabe für die Aktualisierung der Storage-Technologie angeben.

c. Wenn Sie Oracle Real Application Clusters (RAC)-Setup verwenden, können Sie die Speichertechnologie auf einem beliebigen Knoten aktualisieren.

   Das *IsDryRun*-Attribut ist standardmäßig auf true gesetzt. Er identifiziert die Ressourcen, 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 Speicheraktualisierung-API: `/<snapcenter_version>/techrefresh/primarystorage` Oder das Cmdlet: *Invoke-SmTechRefreshPrimaryStorage* aus.

   Dadurch werden die Speicherdetails in den älteren Backups aktualisiert.

   Sie können die API oder das Cmdlet mehrmals auf demselben Host ausführen. Es aktualisiert die Speicherdetails in den älteren Backups nur, wenn der Speicher aktualisiert wird.

   > Die Klonhierarchie kann nicht in ONTAP migriert werden. Verfügt der zu migrierende Storage über geklonte Metadaten in SnapCenter, wird die geklonte Ressource als unabhängige Ressource markiert. Clones von Clone-Metadaten werden rekursiv entfernt.

10. (Optional) Wenn nicht alle Snapshots aus dem alten primären Speicher in den neuen primären Speicher verschoben werden, führen Sie die folgende API aus: `/<snapcenter_version>/hosts/primarybackupsexistencecheck` Oder das Cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    Dadurch wird die Snapshot-Existenzprüfung auf dem neuen primären Speicher durchgeführt und die entsprechenden Backups sind für keinen Vorgang in SnapCenter verfügbar.

Aktualisieren Sie die Backups des sekundären Speichers

Wenn der Speicher aktualisiert wird, sollten Sie die Storage Tech Refresh API oder das Cmdlet ausführen, um die alten Backups in SnapCenter mit den neuen Speicherdetails zu aktualisieren.

Bevor Sie beginnen

Da dieser Workflow die Daten im SnapCenter Repository ändert, wird empfohlen, ein Backup des SnapCenter-Repository zu erstellen. Falls ein Datenprobleme auftreten, kann das SnapCenter Repository mithilfe des Backups in den alten Status zurückgesetzt werden.

Weitere Informationen finden Sie unter "Sichern des SnapCenter Repositorys".

Schritte

1. Migrieren der Daten von altem Storage zu neuem Storage

   Weitere Informationen zur Migration finden Sie unter:

   - "Daten zu neuem Storage migrieren"

- "Wie kann ich ein Volume kopieren und alle Snapshot Kopien beibehalten?"

2. Richten Sie die SnapMirror Beziehung zwischen dem primären Storage und dem neuen sekundären Storage ein, und stellen Sie sicher, dass die Beziehung fehlerfrei ist.
3. Erstellen Sie in SnapCenter ein Backup der Ressourcen, deren Speicher migriert wird.

   SnapCenter benötigt ein neues Backup, um den aktuellen Storage-Platzbedarf zu ermitteln und mit diesem die Metadaten bestehender alter Backups zu aktualisieren.

   > Warten Sie, bis dieser Vorgang abgeschlossen ist. Wenn Sie mit dem nächsten Schritt vor Abschluss fortfahren, verliert SnapCenter die alten sekundären Snapshot Metadaten vollständig.

4. Nachdem alle Ressourcen in einem Host gesichert wurden, führen Sie entweder die sekundäre Speicher-Refresh-API aus: Oder das Cmdlet: `/<snapcenter_version>/techrefresh/secondarystorage` *Invoke-SmTechRefreshSecondaryStorage*.

   Dadurch werden die Details des sekundären Speichers der älteren Backups auf dem angegebenen Host aktualisiert.

   Wenn Sie dies auf Ressourcenebene ausführen möchten, klicken Sie für jede Ressource auf **Aktualisieren**, um die sekundären Speichermetadaten zu aktualisieren.

5. Nach erfolgreicher Aktualisierung der älteren Backups können Sie die alte sekundäre Speicherbeziehung mit 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 mithilfe der SnapCenter-Benutzeroberfläche deinstallieren. Sie können auch einzelne Plug-ins oder Plug-in-Pakete auf Remotehosts mit Hilfe der Befehlszeilenschnittstelle (CLI) auf Ihrem SnapCenter Server Host deinstallieren oder die Windows **Programm deinstallieren** -Option lokal auf einem beliebigen Host verwenden.

Bevor Sie einen Host vom SnapCenter-Server entfernen, müssen Sie die Voraussetzungen erfüllen.

- Melden Sie sich als Administrator an.
- Stellen Sie sicher, dass Ermittlungsjobs nicht auf dem Host ausgeführt werden.
- Sie sollten eine Rolle mit den erforderlichen Berechtigungen zum Entfernen aller mit dem Host verknüpften Objekte zuweisen. Andernfalls schlägt das Entfernen fehl.
- Sie sollten den Fingerabdruck bestätigen, wenn der SSH-Schlüssel nach dem Hinzufügen des Hosts zum SnapCenter geändert wurde.
- Sie sollten den Fingerabdruck bestätigen, wenn der SnapCenter-Host auf eine neuere Version von SnapCenter aktualisiert wird, aber auf dem Plug-in-Host wird noch eine frühere Version des Plug-ins ausgeführt.

Voraussetzungen, um einen Host mithilfe der rollenbasierten Zugriffssteuerung zu entfernen

- Sie sollten sich mit einer RBAC-Rolle angemeldet haben, die über Lese-, Löschen von Host, Installation, Deinstallation von Plug-in und Löschen von Objektberechtigungen verfügt.

  Die Objekte können geklont, gesichert, Ressourcen-Gruppen, Storage-System usw. werden.

- Sie sollten den RBAC-Benutzer zur RBAC-Rolle hinzugefügt haben.
- Sie sollten den RBAC-Benutzer dem Host, Plug-in, Berechtigungen, Ressourcengruppen und dem Storage-System (für Klone) zuweisen, den Sie löschen möchten.
- Sie sollten SnapCenter als RBAC-Benutzer angemeldet haben.

Voraussetzungen zum Entfernen eines Hosts mit Klonen, die aus dem Lebenszyklusvorgang des Klons erstellt wurden

- Sie sollten Klonjobs mit Lifecycle Management von Klonen für SQL Datenbanken erstellt haben.
- Sie sollten eine RBAC-Rolle mit Klon-Lese- und -Löschen, Ressourcen lesen und löschen, Ressourcen-Gruppen lesen und löschen, Storage lesen und löschen, bereitstellen lesen und löschen, mounten, unmounten, Plug-in-Installation und Deinstallation, Host-Lese- und -Löschberechtigungen.
- Sie sollten den RBAC-Benutzer der Rolle RBAC zugewiesen haben.
- Sie sollten den RBAC-Benutzer dem Host, dem SnapCenter Plug-in für Microsoft SQL Server, Zugangsdaten, der Clone Lifecycle Resource Group und dem Storage-System zugewiesen haben.

- Sie sollten SnapCenter als RBAC-Benutzer angemeldet haben.

Entfernen Sie einen Host

Wenn der SnapCenter-Server einen Host entfernt, werden zunächst Backups, Klone, Klonjobs, Ressourcengruppen und Ressourcen, die für diesen Host auf der Seite „SnapCenter-Ressourcen“ aufgeführt sind, entfernt und anschließend die Plug-in-Pakete auf dem Host deinstalliert.

Über diese Aufgabe

- Wenn Sie einen Host löschen, werden auch die Backups, Klone und Ressourcengruppen, die mit dem Host verbunden sind, gelöscht.
- Wenn Sie die Ressourcengruppen entfernen, werden auch alle zugehörigen Zeitpläne entfernt.
- Wenn der Host über eine Ressourcengruppe verfügt, die für einen anderen Host freigegeben ist, und Sie den Host löschen, wird auch die Ressourcengruppe gelöscht.
- Sie sollten das Cmdlet *Remove-SmHost* verwenden, um die nicht mehr verwendeten oder nicht erreichbaren Plug-in-Hosts zu entfernen.

  Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch"

- Die zum Entfernen eines Hosts benötigte Zeit hängt von der Anzahl der Backups und den Aufbewahrungseinstellungen ab. Das liegt daran, dass die Snapshots von jedem 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 die SnapCenter-Software von allen Hosts im Cluster zu entfernen, wählen Sie für Oracle RAC-Cluster die Option **Alle Hosts des Clusters einschließen** aus.

   Sie können auch einen Node eines Clusters entfernen und auf diese Weise alle Nodes nacheinander entfernen.

5. Klicken Sie auf **OK**.

> Wenn Sie Host-Plug-ins auf einem Cluster deinstallieren und neu installieren, werden die Clusterressourcen nicht automatisch erkannt. Wählen Sie den Cluster-Hostnamen aus, und klicken Sie dann auf **Ressourcen aktualisieren**, um die Cluster-Ressourcen automatisch zu ermitteln.

Deinstallieren Sie Plug-ins über die SnapCenter-GUI

Wenn Sie sich entscheiden, dass Sie kein individuelles Plug-in oder ein Plug-in-Paket benötigen, können Sie es über die SnapCenter-Schnittstelle deinstallieren.

Bevor Sie beginnen

- Sie sollten die Ressourcengruppen für das Plug-in-Paket, das Sie deinstallieren, entfernt haben.
- Sie sollten die mit den Ressourcengruppen für das Plug-in-Paket, das Sie deinstallieren, verbundenen Richtlinien losgelöst haben.

Über diese Aufgabe

Sie können ein einzelnes Plug-in deinstallieren. Sie müssen beispielsweise das SnapCenter-Plug-in für Microsoft SQL Server deinstallieren, da einem Host nicht mehr die Ressourcen zur Verfügung stehen und Sie dieses Plug-in auf einen leistungsstärkeren Host verschieben möchten. Sie können auch ein komplettes Plug-in-Paket deinstallieren. Sie müssen beispielsweise das SnapCenter-Plug-ins-Paket für Linux deinstallieren, das SnapCenter-Plug-in für Oracle Database und SnapCenter Plug-in für UNIX umfasst.

- Beim Entfernen eines Hosts werden alle Plug-ins deinstalliert.

  Wenn Sie einen Host aus SnapCenter entfernen, deinstalliert SnapCenter alle Plug-in-Pakete auf dem Host, bevor der Host entfernt wird.

- Dank der SnapCenter GUI werden Plug-ins gleichzeitig von einem Host entfernt.

  Wenn Sie die SnapCenter-Benutzeroberfläche verwenden, können Sie Plug-ins auf nur einem Host gleichzeitig deinstallieren. Sie können jedoch mehrere Deinstallationsvorgänge gleichzeitig ausführen.

  Sie können auch ein Plug-in von mehreren Hosts deinstallieren, indem Sie das Cmdlet *Uninstall-SmHostPackage* und die erforderlichen Parameter verwenden. Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Durch das Deinstallieren des SnapCenter Plug-ins Pakets für Windows von einem Host, auf dem der SnapCenter Server installiert ist, wird die Installation des SnapCenter Servers beschädigt. Deinstallieren Sie das SnapCenter-Plug-ins-Paket für Windows nur dann, wenn Sie sich sicher sind, dass Sie den SnapCenter-Server nicht mehr benötigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite 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**.

Nachdem Sie fertig sind

Sie sollten 5 Minuten warten, bevor Sie das Plug-in auf diesem Host neu installieren. Dieser Zeitraum reicht für die SnapCenter-GUI aus, um den Status des verwalteten Hosts zu aktualisieren. Die Installation schlägt fehl, wenn Sie das Plug-in sofort neu installieren.

Wenn Sie das SnapCenter Plug-ins Package für Linux deinstallieren, finden Sie unter: */Custom_location/snapcenter/log* Deinstallationsdateien.

Deinstallieren Sie Windows Plug-ins mit dem PowerShell Cmdlet

Sie können einzelne Plug-ins deinstallieren oder Plug-ins-Pakete von einem oder mehreren Hosts deinstallieren, indem Sie das Cmdlet *Uninstall-SmHostPackage* auf der

Befehlszeilenschnittstelle des SnapCenter-Servers verwenden.

Sie sollten sich bei SnapCenter als Domänenbenutzer mit lokalen Administratorrechten auf jedem Host, auf dem Sie die Plug-ins deinstallieren möchten, angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Geben Sie auf dem SnapCenter-Server-Host den Befehl *Open-SMConnection -SMSpaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME* ein, und geben Sie dann Ihre Anmeldeinformationen ein.
3. Deinstallieren Sie die Windows-Plug-ins mit dem Cmdlet *Uninstall-SmHostPackage* und den erforderlichen Parametern.

   Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch die "SnapCenter Software Cmdlet Referenzhandbuch".

Deinstallieren Sie Plug-ins lokal auf einem Host

Sie können SnapCenter-Plug-ins lokal auf einem Host deinstallieren, wenn Sie den Host nicht vom SnapCenter-Server erreichen können.

Über diese Aufgabe

Die Best Practice beim Deinstallieren einzelner Plug-ins oder Plug-in-Pakete ist entweder die SnapCenter-Benutzeroberfläche zu verwenden oder das Cmdlet "Uninstall-SmHostPackage" in der Befehlszeilenschnittstelle des SnapCenter-Servers zu verwenden. Diese Verfahren helfen dem SnapCenter-Server, sich mit Änderungen auf dem Laufenden zu halten.

Möglicherweise müssen Sie jedoch Plug-ins nur selten lokal deinstallieren. Sie können beispielsweise einen Deinstallationsauftrag vom SnapCenter-Server ausführen, aber der Job ist fehlgeschlagen, oder Sie haben Ihren SnapCenter-Server deinstalliert und verwaiste Plug-ins bleiben auf einem Host.

Durch die lokale Deinstallation eines Plug-in-Pakets auf einem Host werden die mit dem Host verknüpften Daten nicht gelöscht, z. B. geplante Jobs und Backup-Metadaten.

Versuchen Sie nicht, das SnapCenter-Plug-ins-Paket für Windows lokal von der Systemsteuerung zu deinstallieren. Sie müssen die SnapCenter-Benutzeroberfläche 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 Liste der Programme 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-ins-Paket für Linux oder AIX mithilfe von 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 */Custom_Location/NetApp/snapcenter/spl/Installation/Plugins/uninstall* aus, um die Deinstallation zu starten.

Deinstallieren Sie den SnapCenter-Server auf dem Windows-Host

Wenn Sie den SnapCenter-Server nicht mehr für die Verwaltung von Datensicherungsaufgaben verwenden möchten, können Sie SnapCenter Server mit der Systemsteuerung Programme und Funktionen des SnapCenter-Servers deinstallieren. Durch die Deinstallation des SnapCenter Servers werden alle Komponenten entfernt.

Bevor Sie beginnen

- Stellen Sie sicher, dass mindestens 2 GB freier Speicherplatz auf dem Laufwerk vorhanden ist, auf dem der SnapCenter-Server installiert ist.
- 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 wurde, und versuchen Sie dann, die Deinstallation durchzuführen, schlägt der Vorgang fehl.

- Sie sollten die Repository-Datenbank gesichert haben, da die Repository-Datenbank bereinigt und deinstalliert wird.

Schritte

1. Wechseln Sie auf dem SnapCenter-Server-Host zur Systemsteuerung.
2. Stellen Sie sicher, dass Sie sich in der Ansicht **Kategorie** befinden.
3. Klicken Sie unter Programme auf **Programm deinstallieren**.

   Das Fenster Programme und Funktionen wird geöffnet.

4. Wählen Sie NetApp SnapCenter Server und klicken Sie dann auf **Deinstallieren**.

   Wenn Sie in SnapCenter 4.2 den SnapCenter Server deinstallieren, werden alle Komponenten einschließlich der MySQL Server Repository-Datenbank deinstalliert.

   - Zum Entfernen des NLB-Knotens aus einem NLB-Cluster muss der SnapCenter-Server-Host neu gestartet werden. Wenn Sie den Host nicht neu starten, tritt möglicherweise ein Fehler auf, wenn Sie versuchen, den SnapCenter-Server neu zu installieren.
   - Sie sollten .NET Framework manuell deinstallieren, das während 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 SnapCenter-Server deinstallieren. Durch die Deinstallation des SnapCenter Servers werden alle Komponenten entfernt.

Schritte

1. Führen Sie eine der Aktionen aus, um SnapCenter Server zu deinstallieren.

Wenn Sie Folgendes ausführen möchten:	Tun Sie das…
Nicht interaktive Deinstallation	`$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1` Beispiel: Sudo /opt/NetApp/snapcenter/SnapManagerWeb/Installation/uninstall
Interaktive Deinstallation	`$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall` Geben Sie einen anderen Wert als 0 in die Bestätigungseingabe ein, um die Deinstallation zu bestätigen.

Automatisierung mit REST-APIs

Übersicht ÜBER REST-APIs

REST-APIs können zur Durchführung mehrerer SnapCenter-Managementvorgänge verwendet werden. REST-APIs sind über die Swagger Webseite zugänglich.

Sie können auf die Swagger-Webseite unter *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* zugreifen, um die REST-API-Dokumentation anzuzeigen und einen API-Aufruf manuell auszustellen.

Folgende Plug-ins unterstützen REST-APIs:

- Plug-in für Microsoft SQL Server
- Plug-in für SAP HANA Database
- Plug-in für Oracle Database

Wie kann man nativ auf die SnapCenter REST-API zugreifen

Sie können über jede Programmiersprache, die einen REST-Client unterstützt, direkt auf die SnapCenter REST-API zugreifen. Beliebte Sprachen sind Python, PowerShell und Java.

REST-Web-Services-Grundlage

Representational State Transfer (REST) ist ein Stil für die Erstellung von verteilten Web-Anwendungen. Bei der Anwendung auf das Design einer Web-Services-API werden eine Reihe von Technologien und Best Practices erstellt, um serverbasierte Ressourcen freizulegen und deren Status zu verwalten. Die flexible Grundlage für das Management von SnapCenter bildet mit Mainstream-Protokollen und -Standards.

Ressourcen- und Zustandsdarstellung

Ressourcen sind die Grundkomponenten eines webbasierten Systems. Beim Erstellen einer ANWENDUNG FÜR REST-Webservices umfassen die frühen Designaufgaben Folgendes:

Identifizierung von System- oder serverbasierten Ressourcen

Jedes System nutzt und verwaltet Ressourcen. Eine Ressource kann eine Datei-, Geschäftstransaktion-, Prozess- oder Verwaltungseinheit sein. Eine der ersten Aufgaben bei der Entwicklung einer auf REST-Webservices basierenden Applikation ist die Identifizierung der Ressourcen.

Definition von Ressourcenstatus und zugehörigen Statusoperationen

Die Ressourcen befinden sich immer in einer endlichen Anzahl von Staaten. Die Zustände sowie die damit verbundenen Operationen, die zur Auswirkung der Statusänderungen verwendet werden, sollten klar definiert werden.

URI-Endpunkte

Jede REST-Ressource muss definiert und über ein gut definiertes Adressierungssystem verfügbar gemacht werden. Die Endpunkte, in denen die Ressourcen gefunden und identifiziert werden, verwenden einen einheitlichen Resource Identifier (URI).

Der URI bietet ein allgemeines Framework zum Erstellen eines eindeutigen Namens für jede Ressource im Netzwerk. Der Uniform Resource Locator (URL) ist ein URI-Typ, der mit Webservices zur Identifizierung und zum Zugriff von Ressourcen verwendet wird. Ressourcen werden in der Regel in einer hierarchischen Struktur ausgesetzt, die einem Dateiverzeichnis ähnelt.

HTTP-Meldungen

Hypertext Transfer Protocol (HTTP) ist das Protokoll, das vom Webservice-Client und -Server zum Austausch von Anforderungs- und Antwortmeldungen zu den Ressourcen verwendet wird.

Im Rahmen der Entwicklung einer Web-Services-Anwendung werden HTTP-Methoden den Ressourcen und entsprechenden Statusmanagement-Aktionen zugeordnet. HTTP ist statusfrei. Um im Rahmen einer Transaktion eine Reihe verwandter Anforderungen und Antworten zuzuordnen, müssen daher zusätzliche Informationen in die HTTP-Header enthalten sein, die mit den Anforderungs- und Antwortdatenströmen verwendet werden.

JSON-Formatierung

Während Informationen auf verschiedene Weise zwischen einem Web-Services-Client und Server strukturiert und übertragen werden können, ist die beliebteste Option JavaScript Object Notation (JSON).

JSON ist ein Branchenstandard für die Darstellung einfacher Datenstrukturen im Klartext und wird zur Übertragung von Zustandsdaten zur Beschreibung der Ressourcen verwendet. Die SnapCenter REST API verwendet JSON, um die Daten zu formatieren, die im Körper jeder HTTP-Anfrage und Antwort verwendet werden.

Grundlegende betriebliche Eigenschaften

IM RUHEZUSTAND werden einheitliche Technologien und Best Practices erstellt, jedoch können die Details jeder API je nach dem verfügbaren Design variieren.

API-Transaktion bei Anfrage und Reaktion

Jeder REST-API-Aufruf wird als HTTP-Anfrage an das SnapCenter-Serversystem durchgeführt, das eine entsprechende Antwort auf den Client generiert. Dieses Anforderungs- und Antwortpaar wird als API-Transaktion betrachtet.

Bevor Sie die API verwenden, sollten Sie mit den verfügbaren Eingabevariablen zur Steuerung einer Anfrage und dem Inhalt der Antwortausgabe vertraut sein.

Unterstützung von CRUD-Vorgängen

Auf alle über das SnapCenter REST API verfügbaren Ressourcen kann basierend auf dem CRUD-Modell zugegriffen werden:

- Erstellen

- Lesen
- Aktualisieren
- Löschen

Für einige der Ressourcen wird nur ein Teil der Vorgänge unterstützt.

Objektkennungen

Jeder Ressourceninstanz oder jedem Objekt wird eine eindeutige Kennung zugewiesen, wenn sie erstellt wird. In den meisten Fällen ist die Kennung eine 128-Bit-UUID. Diese Kennungen sind global eindeutig in einem bestimmten SnapCenter-Server.

Nachdem ein API-Aufruf ausgegeben wurde, der eine neue Objektinstanz erstellt, wird eine URL mit der zugehörigen ID an den Anrufer in der Kopfzeile der HTTP-Antwort zurückgegeben. Sie können die Kennung extrahieren und bei nachfolgenden Anrufen verwenden, wenn Sie sich auf die Ressourceninstanz beziehen.

Der Inhalt und die interne Struktur der Objektkennungen können jederzeit geändert werden. Wenn Sie auf die zugeordneten Objekte verweisen, sollten Sie die Kennungen für die entsprechenden API-Aufrufe nur nach Bedarf verwenden.

Objektinstanzen und -Sammlungen

Je nach Ressourcenpfad und HTTP-Methode kann ein API-Aufruf auf eine bestimmte Objektinstanz oder eine Sammlung von Objekten angewendet werden.

Synchroner und asynchroner Betrieb

SnapCenter führt eine HTTP-Anforderung durch, die von einem Client entweder synchron oder asynchron empfangen wird.

Synchrone Verarbeitung

SnapCenter führt die Anfrage sofort aus und antwortet mit einem HTTP-Statuscode von 200 oder 201, wenn er erfolgreich ist.

Jede Anfrage, die die Methode GET verwendet, wird immer synchron ausgeführt. Zusätzlich sind Anfragen, die POST verwenden, so ausgelegt, dass sie synchron ausgeführt werden können, wenn sie in weniger als zwei Sekunden abgeschlossen sein sollen.

Asynchrone Verarbeitung

Wenn eine asynchrone Anforderung gültig ist, erstellt SnapCenter eine Hintergrundaufgabe zur Verarbeitung der Anforderung und ein Jobobjekt zum Anker der Aufgabe. Der HTTP-Statuscode 202 wird zusammen mit dem Jobobjekt an den Anrufer zurückgegeben. Sie sollten den Status des Jobs abrufen, um den Erfolg oder den Fehler zu ermitteln.

Anfragen, die DIE POST- und LÖSCHMETHODEN verwenden, werden asynchron ausgeführt, wenn dies voraussichtlich mehr als zwei Sekunden dauert.

Sicherheit

Die Sicherheit der REST-API basiert in erster Linie auf den vorhandenen Sicherheitsfunktionen von

SnapCenter. Die folgende Sicherheit wird von der API verwendet:

Sicherheit In Transportschicht

Der gesamte über das Netzwerk zwischen dem SnapCenter-Server und dem Client gesendete Datenverkehr wird basierend auf den SnapCenter-Konfigurationseinstellungen in der Regel mit TLS verschlüsselt.

HTTP-Authentifizierung

Auf HTTP-Ebene wird die grundlegende Authentifizierung für die API-Transaktionen verwendet. Jeder Anforderung wird ein HTTP-Header mit dem Benutzernamen und Passwort in einem Base64-String hinzugefügt.

Eingabevariablen, die eine API-Anforderung steuern

Sie können steuern, wie ein API-Aufruf über Parameter und Variablen verarbeitet wird, die in der HTTP-Anforderung festgelegt sind.

HTTP-Methoden

Die von der SnapCenter REST API unterstützte HTTP-Methoden sind in der folgenden Tabelle aufgeführt.

Nicht alle HTTP-Methoden sind an jedem REST-Endpunkt verfügbar.

HTTP-Methode	Beschreibung
GET	Ruft Objekteigenschaften auf einer Ressourceninstanz oder -Sammlung ab.
POST	Erstellt eine neue Ressourceninstanz basierend auf der angegebenen Eingabe.
Löschen	Löscht eine vorhandene Ressourceninstanz.
PUT	Ändert eine vorhandene Ressourceninstanz.

Anfragekopfzeilen

Sie sollten mehrere Header in die HTTP-Anfrage aufnehmen.

Inhaltstyp

Wenn der Anforderungsinstanz JSON enthält, sollte dieser Header auf *Application/json* gesetzt werden.

Akzeptieren

Dieser Header sollte auf *Application/json* gesetzt werden.

Autorisierung

Die grundlegende Authentifizierung sollte mit dem Benutzernamen und dem Passwort als base64-Zeichenfolge codiert werden.

Text anfordern

Der Inhalt der Anfraentext variiert je nach Anruf. Der HTTP-Request-Text besteht aus einem der folgenden Elemente:

- JSON-Objekt mit Eingabevariablen
- Leer

Objekte filtern

Wenn Sie einen API-Aufruf ausgeben, der GET verwendet, können Sie die zurückgegebenen Objekte anhand eines beliebigen Attributs einschränken oder filtern. Sie können beispielsweise einen genauen Wert angeben, der übereinstimmt:

```
<field>=<query value>
```

Neben einer genauen Übereinstimmung stehen auch andere Operatoren zur Verfügung, um einen Satz von Objekten über einen Wertebereich zurückzugeben. Die SnapCenter REST API unterstützt die in der nachfolgenden Tabelle aufgeführten Filteroperatoren.

Operator	Beschreibung
=	Gleich
<	Kleiner als
>	Größer als
≪=	Kleiner oder gleich
>=	Größer oder gleich
AKTUALISIERUNG	Oder
!	Nicht gleich
*	Gierige Wildcard

Sie können auch eine Sammlung von Objekten zurückgeben, basierend darauf, ob ein bestimmtes Feld gesetzt wird oder nicht, indem Sie das Schlüsselwort **Null** oder dessen Negation **!null** als Teil der Abfrage verwenden.

Nicht festgelegte Felder werden in der Regel von übereinstimmenden Abfragen ausgeschlossen.

Es werden bestimmte Objektfelder angefordert

Standardmäßig gibt die Ausgabe eines API-Aufrufs mithilfe VON GET nur die Attribute zurück, die das Objekt oder die Objekte eindeutig identifizieren. Dieser minimale Feldsatz dient als Schlüssel für jedes Objekt und variiert je nach Objekttyp. Sie können mithilfe des Abfrageparameters weitere Objekteigenschaften wie folgt auswählen `fields` :

Allgemeine oder Standardfelder

Geben Sie **Fields=*** an, um die am häufigsten verwendeten Objektfelder abzurufen. Diese Felder werden normalerweise im lokalen Serverspeicher verwaltet oder erfordern nur wenig Verarbeitung für den Zugriff. Dies

sind die gleichen Eigenschaften, die für ein Objekt zurückgegeben werden, nachdem GET mit einem URL-Pfadschlüssel (UUID) verwendet wurde.

Alle Felder

Geben Sie **fields=**** an, um alle Objektfelder abzurufen, einschließlich derer, die für den Zugriff auf zusätzliche Serververarbeitung erforderlich sind.

Benutzerdefinierte Feldauswahl

Geben Sie mit **fields=<field_Name>** das genaue Feld ein. Wenn Sie mehrere Felder anfordern, müssen die Werte durch Kommas ohne Leerzeichen getrennt werden.

> Als Best Practice sollten Sie immer die gewünschten Felder identifizieren. Sie sollten nur die gemeinsamen Felder oder alle Felder abrufen, wenn Sie dies benötigen. Welche Felder sind als „Common“ klassifiziert und mit *fields=** zurückgegeben werden, wird durch NetApp aufgrund der internen Performance-Analyse bestimmt. Die Klassifizierung eines Felds kann sich in zukünftigen Releases ändern.

Sortieren von Objekten im Ausgabungsset

Die Datensätze in einer Ressourcensammlung werden in der vom Objekt definierten Standardreihenfolge zurückgegeben. Sie können die Reihenfolge mit dem Abfrageparameter mit dem Feldnamen und der Sortierrichtung wie folgt ändern `order_by` :

```
order_by=<field name> asc|desc
```

Sie können beispielsweise das Typfeld in absteigender Reihenfolge, gefolgt von 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 eingeben, müssen Sie die Felder mit einem Komma trennen.

Paginierung beim Abrufen von Objekten in einer Sammlung

Wenn ein API-Aufruf über GET auf eine Sammlung von Objekten desselben Typs zugreifen soll, versucht SnapCenter, auf der Grundlage von zwei Einschränkungen so viele Objekte wie möglich zurückzugeben. Mit zusätzlichen Abfrageparametern auf der Anforderung können Sie jede dieser Einschränkungen steuern. Die erste Bedingung, die für eine bestimmte GET-Anforderung erreicht wurde, beendet die Anforderung und begrenzt damit die Anzahl der zurückgegebenen Datensätze.

> Wenn eine Anfrage endet, bevor sie alle Objekte anführt, enthält die Antwort den Link, der zum Abrufen des nächsten Stapels von Datensätzen benötigt wird.

Die Anzahl der Objekte wird begrenzt

Standardmäßig gibt SnapCenter maximal 10,000 Objekte für EINE GET-Anforderung aus. Sie können diese Grenze mit dem Abfrageparameter *max_Records* ändern. Beispiel:

```
max_records=20
```

Die Anzahl der tatsächlich zurückgegebenen Objekte kann aufgrund der entsprechenden Zeitbeschränkung sowie der Gesamtanzahl der Objekte im System kleiner sein als die maximale Wirkung.

Begrenzung der Zeit, die zum Abrufen der Objekte verwendet wird

Standardmäßig gibt SnapCenter so viele Objekte wie möglich innerhalb der für die GET-Anforderung zulässigen Zeit zurück. Die Standard-Zeitüberschreitung beträgt 15 Sekunden. Sie können diese Grenze mit dem Abfrageparameter *return_timeout* ändern. Beispiel:

```
return_timeout=5
```

Die Anzahl der tatsächlich zurückgegebenen Objekte kann aufgrund der damit verbundenen Beschränkung auf die Anzahl der Objekte sowie die Gesamtanzahl der Objekte im System kleiner sein als die maximal zulässige Anzahl.

Verengung des Ergebnisset

Bei Bedarf können Sie diese beiden Parameter mit zusätzlichen Abfrageparametern kombinieren, um den Ergebnissatz einzugrenzen. Im Folgenden werden z. B. bis zu 10 EMS-Ereignisse zurückgegeben, die nach der angegebenen Zeit generiert wurden:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Sie können mehrere Anfragen zur Seite durch die Objekte ausgeben. Jeder nachfolgende API-Aufruf sollte einen neuen Zeitwert verwenden, der auf dem letzten Ereignis des letzten Ergebnisset basiert.

Größeneigenschaften

Die bei einigen API-Aufrufen verwendeten Eingabewerte sowie bestimmte Abfrageparameter sind numerisch. Anstatt eine ganze Zahl in Byte bereitzustellen, können Sie optional ein Suffix wie in der folgenden Tabelle aufgeführt verwenden.

Suffix	Beschreibung
KB	KB-Kilobyte (1024 Byte) oder Kibibyte
MB	MB Megabyte (KB x 1024 Byte) oder Mebibyte
GB	GB Gigabyte (MB x 1024 Byte) oder Gibibyte
TB	TB Terabyte (GB x 1024 byes) oder Tebibyte
PB	PB (TB x 1024 byes) oder Pebibyte

Interpretation einer API-Antwort

Jede API-Anfrage generiert eine Antwort an den Client. Sie sollten die Antwort überprüfen, um festzustellen, ob sie erfolgreich war, und weitere Daten nach Bedarf abrufen.

HTTP-Statuscode

Im Folgenden werden die von der SnapCenter REST API verwendeten HTTP-Statuscodes beschrieben.

Codieren	Beschreibung
200	OK zeigt Erfolg für Anrufe an, die kein neues Objekt erstellen.
201	Ein Objekt wurde erfolgreich erstellt. Der Positionskopf in der Antwort enthält die eindeutige Kennung für das Objekt.
202	Angenommen Ein Hintergrundjob wurde gestartet, um die Anfrage auszuführen, wurde aber noch nicht abgeschlossen.
400	Ungültige Anfrage die Eingabe der Anforderung wurde nicht erkannt oder ist nicht angemessen.
401	Nicht autorisierte Benutzerauthentifizierung fehlgeschlagen.
403	Aufgrund eines Autorisierungsfehlers (RBAC) wird der Zugriff verweigert.
404	Die Ressource, auf die in der Anfrage verwiesen wird, wurde nicht gefunden.
405	Methode nicht zulässig die HTTP-Methode in der Anfrage 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 Beim Server ist ein allgemeiner interner Fehler aufgetreten.

Antwortkopfzeilen

In der vom SnapCenter erzeugten HTTP-Antwort sind mehrere Header enthalten.

Standort

Wenn ein Objekt erstellt wird, enthält die Standortkopfzeile die komplette URL zum neuen Objekt einschließlich der eindeutigen Kennung, die dem Objekt zugewiesen ist.

Inhaltstyp

Dies wird in der Regel sein `application/json`.

Antwortkörper

Der Inhalt des Antwortkörpers, der sich aus einer API-Anfrage ergibt, unterscheidet sich je nach Objekt, Verarbeitungstyp und Erfolg oder Misserfolg der Anforderung. Die Antwort wird immer in JSON gerendert.

Einzelnes Objekt

Je nach Anforderung kann ein einzelnes Objekt mit einer Reihe von Feldern zurückgegeben werden. Beispielsweise können Sie GET verwenden, um ausgewählte Eigenschaften eines Clusters mit der eindeutigen Kennung abzurufen.

Mehrere Objekte

Es können mehrere Objekte aus einer Ressourcensammlung zurückgegeben werden. In jedem Fall wird ein konsistentes Format verwendet, in dem `num_records` die Anzahl der Datensätze und Datensätze angegeben wird, die ein Array der Objektinstanzen enthalten. Beispielsweise können Sie die in einem bestimmten Cluster definierten Nodes abrufen.

Jobobjekt

Wenn ein API-Aufruf asynchron verarbeitet wird, wird ein Job-Objekt zurückgegeben, das den Hintergrund-Task ankers. Beispielsweise wird die PATCH-Anfrage, die zum Aktualisieren der Cluster-Konfiguration verwendet wird, asynchron verarbeitet und ein Job-Objekt zurückgegeben.

Fehlerobjekt

Wenn ein Fehler auftritt, wird immer ein Fehlerobjekt zurückgegeben. Beispielsweise erhalten Sie einen Fehler beim Versuch, ein Feld zu ändern, das nicht für ein Cluster definiert ist.

Leer

In bestimmten Fällen werden keine Daten zurückgegeben und der Antwortkörper enthält ein leeres JSON-Objekt.

Fehler

Wenn ein Fehler auftritt, wird ein Fehlerobjekt im Antwortkörper zurückgegeben.

Formatieren

Ein Fehlerobjekt hat das folgende Format:

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

Sie können den Codewert verwenden, um den allgemeinen Fehlertyp oder die allgemeine Fehlerkategorie zu bestimmen, und die Meldung, um den spezifischen Fehler zu ermitteln. Wenn verfügbar, enthält das Zielfeld die spezifische Benutzereingabe, die mit dem Fehler verknüpft ist.

Allgemeine Fehlercodes

Die gängigen Fehlercodes werden in der folgenden Tabelle beschrieben. Spezifische API-Aufrufe können zusätzliche Fehlercodes enthalten.

Codieren	Beschreibung
409	Ein Objekt mit derselben Kennung ist bereits vorhanden.
400	Der Wert für ein Feld hat einen ungültigen Wert oder fehlt oder es wurde ein zusätzliches Feld angegeben.
400	Der Vorgang wird nicht unterstützt.
405	Ein Objekt mit der angegebenen Kennung wurde nicht gefunden.
403	Die Berechtigung zur Durchführung der Anforderung wird verweigert.
409	Die Ressource wird verwendet.

REST-APIs werden für SnapCenter Server und Plug-ins unterstützt

Die über die SnapCenter REST API verfügbaren Ressourcen sind nach Kategorien sortiert, die auf der Dokumentationsseite der SnapCenter-API angezeigt werden. Nachfolgend finden Sie eine kurze Beschreibung der einzelnen Ressourcen mit den grundlegenden Ressourcenpfaden sowie weitere Nutzungsüberlegungen.

Auth

Sie können diese API verwenden, um sich beim SnapCenter-Server anzumelden. Diese API gibt ein Benutzerautorisierungs-Token zurück, das zur Authentifizierung weiterer Anforderungen verwendet wird.

Domänen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie alle Domänen in SnapCenter ab
- Abrufen von Details einer bestimmten Domäne
- Registrieren oder Aufheben der Registrierung einer Domain
- Ändern einer Domäne

Jobs

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie alle Jobs in SnapCenter ab
- Abrufen des Status eines Jobs
- Einen Job abbrechen oder beenden

Einstellungen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Registrieren, Ändern oder Entfernen von Anmeldeinformationen
- Zeigt die Anmeldeinformationen an, die auf dem SnapCenter-Server registriert sind
- Benachrichtigungseinstellungen konfigurieren
- Ruft Informationen über den SMTP-Server ab, der derzeit für das Senden 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-Serveranmeldung an
- Aktivieren oder Deaktivieren und Konfigurieren von MFA für die SnapCenter-Server-Anmeldung
- Erstellen Sie die zum Einrichten von MFA erforderliche Konfigurationsdatei

Hosts

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Abfrage aller SnapCenter-Hosts
- Entfernen Sie einen oder mehrere Hosts aus SnapCenter
- Rufen Sie einen Host nach Namen ab
- Rufen Sie alle Ressourcen auf einem Host ab
- Rufen Sie eine Ressource mithilfe der Ressourcen-ID ab
- Rufen Sie die Plug-in-Konfigurationsdetails ab
- Konfigurieren Sie den Plug-in-Host
- Rufen Sie alle Ressourcen des Plug-ins für Microsoft SQL Server Host ab
- Rufen Sie alle Ressourcen des Plug-ins für Oracle Datenbank-Host ab
- Rufen Sie alle Ressourcen des Plug-ins für benutzerdefinierten Applikations-Host ab
- Rufen Sie alle Ressourcen des Plug-ins für SAP HANA-Host ab
- Abrufen der installierten Plug-ins
- Installieren von Plug-ins auf einem vorhandenen Host
- Hostpaket wird aktualisiert
- Entfernen Sie Plug-ins von einem vorhandenen Host
- Fügen Sie Plug-in auf einem Host hinzu
- Fügen Sie einen Host hinzu oder ändern Sie diesen
- Holen Sie sich die Signatur des Linux-Hosts
- Registrieren Sie die Signatur des Linux-Hosts
- Versetzen Sie den Host in den Wartungs- oder Produktionsmodus
- Starten oder starten Sie die Plug-in-Dienste auf dem Host neu
- Benennen Sie einen Host um

Ressourcen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie alle Ressourcen ab
- Rufen Sie eine Ressource mithilfe der Ressourcen-ID ab
- Rufen Sie alle Ressourcen des Plug-ins für Microsoft SQL Server Host ab
- Rufen Sie alle Ressourcen des Plug-ins für Oracle Datenbank-Host ab
- Rufen Sie alle Ressourcen des Plug-ins für benutzerdefinierten Applikations-Host ab
- Rufen Sie alle Ressourcen des Plug-ins für SAP HANA-Host ab
- Rufen Sie eine Microsoft SQL Server-Ressource mit einem Schlüssel ab
- Abrufen einer benutzerdefinierten Ressource mit einem Schlüssel
- Ändern Sie eine Ressource des Plug-ins für benutzerdefinierten Applikations-Host
- Entfernen Sie mithilfe eines Schlüssels eine Ressource des Plug-ins für benutzerdefinierten Applikations-Host
- Abrufen einer SAP HANA-Ressource mit einem Schlüssel
- Änderung einer Ressource des Plug-ins für SAP HANA-Host
- Entfernen Sie eine Ressource des Plug-ins für SAP HANA-Host mithilfe eines Schlüssels
- Rufen Sie eine Oracle-Ressource mit einem Schlüssel ab
- Erstellen einer Oracle Application Volume-Ressource
- Bearbeiten einer Oracle Application Volume-Ressource
- Entfernen Sie eine Oracle Application Volume-Ressource mit einem Schlüssel
- Rufen Sie die sekundären Details der Oracle-Ressource ab
- Sichern Sie die Microsoft SQL Server-Ressource mit einem Plug-in für Microsoft SQL Server
- Sichern Sie die Oracle Ressource mit Plug-in für Oracle Database
- Sichern Sie die benutzerdefinierte Ressource mit Plug-in für benutzerdefinierte Applikationen
- SAP HANA-Datenbank konfigurieren
- Konfigurieren Sie die Oracle Datenbank
- Wiederherstellen eines Backups einer SQL-Datenbank
- Wiederherstellen eines Backups einer Oracle Datenbank
- Wiederherstellung eines Backups benutzerdefinierter Applikationen
- SAP HANA-Ressource erstellen
- Schützen Sie eine benutzerdefinierte Ressource mit Plug-in für benutzerdefinierte Applikationen
- Schützen Sie eine Microsoft SQL Server-Ressource mit Plug-in für Microsoft SQL Server
- Ändern einer geschützten Microsoft SQL Server-Ressource
- Entfernen Sie den Schutz für Microsoft SQL Server-Ressourcen
- Schutz einer Oracle-Ressource über Plug-in für Oracle Datenbank
- Geschützte Oracle-Ressource ändern
- Entfernen Sie Schutz aus Oracle-Ressource
- Klonen Sie eine Ressource aus dem Backup mit Plug-in für benutzerdefinierte Applikationen
- Klonen eines Oracle Applikations-Volumes aus dem Backup mit Plug-in für Oracle Database

- Klonen einer Microsoft SQL Server-Ressource aus dem Backup mit dem Plug-in für Microsoft SQL Server
- Erstellen Sie den Lebenszyklus eines Klons einer Microsoft SQL Server Ressource
- Ändern Sie den Lebenszyklus des Klons einer Microsoft SQL Server-Ressource
- Löschen Sie den Lebenszyklus des Klons einer Microsoft SQL Server-Ressource
- Verschieben Sie eine vorhandene Microsoft SQL Server Datenbank von einer lokalen Festplatte auf eine NetApp LUN
- Erstellen Sie eine Clone Specification File für eine Oracle Database
- Initiieren eines On-Demand-Klonaktualisierungsauftrags für eine Oracle Ressource
- Erstellen Sie eine Oracle-Ressource aus dem Backup mit der Clone Specification File
- Stellt die Datenbank auf dem sekundären Replikat wieder her und schließt die Datenbank wieder der Verfügbarkeitsgruppe an
- Erstellen einer Oracle Application Volume-Ressource

Backups

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Abrufen von Backup-Details nach Backup-Name, Typ, Plug-in, Ressource oder Datum
- Rufen Sie alle Backups ab
- Rufen Sie Backup-Details ab
- Backups umbenennen oder löschen
- Mounten Sie ein Oracle Backup
- Heben Sie die Bereitstellung eines Oracle Backups auf
- Katalogisieren eines Oracle Backups
- Entkatalogisieren eines Oracle Backups
- Abrufen aller erforderlichen Backups zum Ausführen eines Point-in-Time Recovery

Klone

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Erstellen, Anzeigen, Ändern und Löschen der Spezifikationsdatei für Oracle-Datenbankklone
- Anzeigen der Oracle-Datenbankklonhierarchie
- Abrufen von Klondetails
- Rufen Sie alle Klone ab
- Klone löschen
- Rufen Sie Klondetails nach ID ab
- Initiieren eines On-Demand-Klonaktualisierungsauftrags für eine Oracle Ressource
- Klonen einer Oracle-Ressource aus dem Backup mit der Clone Specification File

Aufteilung klonen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Schätzen Sie den Abteilungvorgang für den Klon der geklonten Ressource
- Abrufen des Status eines geteilten Klonvorgangs
- Starten oder stoppen Sie einen Klon-Split-Vorgang

Ressourcengruppen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Abrufen von Details aller Ressourcengruppen
- Rufen Sie die Ressourcengruppe nach Namen ab
- Erstellen Sie eine Ressourcengruppe für das Plug-in für benutzerdefinierte Anwendungen
- Erstellen Sie eine Ressourcengruppen für das Plug-in für Microsoft SQL Server
- Erstellen Sie eine Ressourcengruppe für das Plug-in für Oracle-Datenbank
- Ändern Sie eine Ressourcengruppe für das Plug-in für benutzerdefinierte Anwendungen
- Ändern Sie eine Ressourcengruppe für das Plug-in für Microsoft SQL Server
- Ändern Sie eine Ressourcengruppe für das Plug-in für Oracle-Datenbank
- Erstellen, Ändern oder Löschen des Klonlebenszyklus einer Ressourcengruppe für das Plug-in für Microsoft SQL Server
- Sichern einer Ressourcengruppe
- Setzen Sie die Ressourcengruppe in den Wartungs- oder Produktionsmodus
- Entfernen Sie eine Ressourcengruppe

Richtlinien

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Abrufen von Richtliniendetails
- Richtliniendetails nach Namen abrufen
- Löschen einer Richtlinie
- Erstellen einer Kopie einer vorhandenen Richtlinie
- Erstellen oder Ändern Sie eine Richtlinie für das Plug-in für benutzerdefinierte Applikationen
- Erstellen oder Ändern Sie die Richtlinie für das Plug-in für Microsoft SQL Server
- Erstellen oder Ändern Sie eine Richtlinie für das Plug-in für Oracle Database
- Erstellen oder Ändern Sie eine Richtlinie für das Plug-in für die SAP HANA Datenbank

Storage

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie alle Freigaben ab

- Freigabe nach Namen abrufen
- Erstellen oder Löschen einer Freigabe
- Abrufen von Storage-Details
- Speicherdetails nach Namen abrufen
- Erstellen, Ändern oder Löschen von Speicher
- Erkennung von Ressourcen auf einem Storage-Cluster
- Abrufen von Ressourcen auf einem Storage-Cluster

Share

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie die Details einer Freigabe ab
- Rufen Sie die Details aller Freigaben ab
- Erstellen oder löschen Sie eine Freigabe auf dem Speicher
- Freigabe nach Namen abrufen

Plug-Ins

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Listen Sie alle Plug-ins für einen Host auf
- Rufen Sie eine Microsoft SQL Server-Ressource mit einem Schlüssel ab
- Ändern Sie eine benutzerdefinierte Ressource mit einem Schlüssel
- Entfernen Sie eine benutzerdefinierte Ressource mit einem Schlüssel
- Abrufen einer SAP HANA-Ressource mit einem Schlüssel
- Ändern einer SAP HANA-Ressource mit einem Schlüssel
- Entfernen einer SAP HANA-Ressource mithilfe eines Schlüssels
- Rufen Sie eine Oracle-Ressource mit einem Schlüssel ab
- Ändern Sie eine Oracle Application Volume-Ressource mit einem Schlüssel
- Entfernen Sie eine Oracle Application Volume-Ressource mit einem Schlüssel
- Sichern Sie die Microsoft SQL Server-Ressource mit Plug-in für Microsoft SQL Server und einem Schlüssel
- Sichern Sie die Oracle-Ressource mit Plug-in für Oracle Database und einem Schlüssel
- Sichern Sie die benutzerdefinierte Applikationsressource mithilfe eines Plug-ins für benutzerdefinierte Applikationen und einen Schlüssel
- SAP HANA-Datenbank mit einem Schlüssel konfigurieren
- Konfigurieren Sie die Oracle-Datenbank mit einem Schlüssel
- Wiederherstellung eines Backups benutzerdefinierter Applikationen mit einem Schlüssel
- SAP HANA-Ressource erstellen
- Erstellen einer Oracle Application Volume-Ressource

- Schützen Sie eine benutzerdefinierte Ressource mit Plug-in für benutzerdefinierte Applikationen
- Schützen Sie eine Microsoft SQL Server-Ressource mit Plug-in für Microsoft SQL Server
- Ändern einer geschützten Microsoft SQL Server-Ressource
- Entfernen Sie den Schutz für Microsoft SQL Server-Ressourcen
- Schutz einer Oracle-Ressource über Plug-in für Oracle Datenbank
- Geschützte Oracle-Ressource ändern
- Entfernen Sie Schutz aus Oracle-Ressource
- Klonen Sie eine Ressource aus dem Backup mit Plug-in für benutzerdefinierte Applikationen
- Klonen eines Oracle Applikations-Volumes aus dem Backup mit Plug-in für Oracle Database
- Klonen einer Microsoft SQL Server-Ressource aus dem Backup mit dem Plug-in für Microsoft SQL Server
- Erstellen Sie den Lebenszyklus eines Klons einer Microsoft SQL Server Ressource
- Ändern Sie den Lebenszyklus des Klons einer Microsoft SQL Server-Ressource
- Löschen Sie den Lebenszyklus des Klons einer Microsoft SQL Server-Ressource
- Erstellen Sie eine Clone Specification File für eine Oracle Database
- Initiieren eines On-Demand-Klonzyklus einer Oracle Ressource
- Klonen einer Oracle-Ressource aus dem Backup mit der Clone Specification File

Berichte An

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Abrufen von Berichten über Backup, Wiederherstellung und Klonvorgänge für die jeweiligen Plug-ins
- Hinzufügen, Ausführen, Löschen oder Ändern von Zeitplänen
- Abrufen von Daten für die geplanten Berichte

Meldungen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie alle Meldungen ab
- Abrufen von Warnmeldungen nach IDs
- Löschen Sie mehrere Warnmeldungen oder löschen Sie eine Meldung nach ID

Rbac

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Abrufen von Details zu Benutzern, Gruppen und Rollen
- Benutzer hinzufügen oder löschen
- Benutzer der Rolle zuweisen
- Heben Sie die Zuweisung von Benutzer aus Rolle auf
- Erstellen, Ändern oder Löschen von Rollen

- Gruppe einer Rolle zuweisen
- Heben Sie die Zuordnung einer Gruppe zu einer Rolle auf
- Gruppen hinzufügen oder löschen
- Erstellen Sie eine Kopie einer vorhandenen Rolle
- Weisen Sie dem Benutzer oder der Gruppe Ressourcen zu oder heben Sie die Zuweisung zurück

Konfiguration

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Zeigen Sie die Konfigurationseinstellungen an
- Ändern Sie die Konfigurationseinstellungen

Zertifikateinstellungen

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Zeigen Sie den Zertifikatsstatus für den SnapCenter-Server oder den Plug-in-Host an
- Ändern Sie die Zertifikatseinstellungen für den SnapCenter-Server oder den Plug-in-Host

Repository

Mit APIs können unterschiedliche Vorgänge durchgeführt werden.

- Rufen Sie die Repository-Backups ab
- Zeigen Sie die Konfigurationsinformationen zum Repository an
- Sichern und Wiederherstellen des SnapCenter Repositorys
- Heben Sie den Schutz des SnapCenter Repositorys auf
- Wiederherstellung und Failover des Repositorys

Version

Sie können diese API zum Anzeigen der SnapCenter-Version verwenden.

Zugriff auf REST-APIs über die Swagger API-Webseite

REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um die REST-APIs des SnapCenter-Servers anzuzeigen und einen API-Aufruf manuell auszuführen. MIT REST-APIs können Sie Ihren SnapCenter Server managen oder Datensicherungsvorgänge ausführen.

Sie sollten die Management-IP-Adresse oder den Domain-Namen des SnapCenter Servers kennen, auf dem Sie die REST-APIs ausführen möchten.

Für die Ausführung des REST-API-Clients sind keine speziellen Berechtigungen erforderlich. Jeder Benutzer kann auf die Swagger Webseite zugreifen. Die entsprechenden Berechtigungen für die Objekte, auf die über DIE REST-API zugegriffen wird, basieren auf dem Benutzer, der das Token generiert, um sich bei DER REST-API anzumelden.

Schritte

1. Geben Sie in einem Browser die URL für den 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 hat: +, ., % und &.

2. Wenn die Dokumentation der Swagger-API 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 **Entdecken**.

   Es wird eine Liste der API-Ressourcentypen oder -Kategorien angezeigt.

4. Klicken Sie auf einen API-Ressourcentyp, um die APIs in diesem Ressourcentyp anzuzeigen.

Wenn bei der Ausführung von SnapCenter REST-APIs unerwartetes Verhalten auftritt, können Sie mithilfe der Protokolldateien die Ursache identifizieren und das Problem beheben. Sie können die Protokolldateien von der SnapCenter Benutzeroberfläche herunterladen, indem Sie auf **Monitor** > **Protokolle** > **Download** klicken.

Legen Sie los mit DER REST API

Die SnapCenter REST API ist ein schneller Einstieg. Der Zugriff auf die API bietet eine gewisse Perspektive, bevor Sie mit den komplexeren Workflow-Prozessen bei Live-Einrichtung beginnen.

Hallo Welt

Sie können einen einfachen Befehl auf Ihrem System ausführen, um die SnapCenter REST API zu verwenden und deren 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 Passwort für ein Konto mit Berechtigung für den Zugriff auf die SnapCenter REST API.

Wenn Ihre Anmeldeinformationen Sonderzeichen enthalten, müssen Sie diese auf der Grundlage der verwendeten Shell so formatieren, dass sie für Curl akzeptabel sind. Sie können beispielsweise vor jedem Sonderzeichen einen umgekehrten Schrägstrich einfügen oder die gesamte Zeichenfolge in einfache Anführungszeichen umbrechen `username:password`.

Schritt

Führen Sie bei 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 ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"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 der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis für SnapCenter 6.0"