SnapManager 3.4.2 für Oracle

SnapManager Oracle

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapmanager-oracle/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

SnapManager 3.4.2 für Oracle . . . 1
Versionshinweise zu SnapManager 3.4.2 für Oracle . . . 2
Installations- und Setup-Handbuch für UNIX® . . . 3
Produktübersicht . . . 3
SnapManager Highlights . . . 3
Architektur von SnapManager . . . 4
Implementierungs-Workflow . . . 5
Bereitstellung wird vorbereitet . . . 6
SnapManager Lizenzierung . . . 7
Unterstützte Konfigurationen . . . 8
Unterstützte Speichertypen . . . 8
UNIX Host-Anforderungen . . . 9
Datenbanken werden konfiguriert . . . 9
Konfigurieren der Zieldatenbank . . . 9
Erstellen eines Oracle-Datenbankbenutzers für die Zieldatenbank . . . 9
Erstellen der Repository-Datenbankinstanz . . . 10
Erstellen eines Oracle-Benutzers für die Repository-Datenbankinstanz . . . 10
Überprüfen der Oracle Listener-Konfiguration . . . 11
SnapManager wird installiert . . . 11
Einrichtung von SnapManager . . . 12
Starten des SnapManager-Servers . . . 12
Zugriff auf die SnapManager Benutzeroberfläche . . . 13
SnapManager-Repository wird konfiguriert . . . 13
Vorbereiten der Speichersysteme für die SnapMirror- und SnapVault-Replizierung . . . 14
Verständnis der Unterschiede zwischen SnapMirror und SnapVault . . . 15
Vorbereiten der Storage-Systeme für die SnapMirror Replizierung . . . 15
Storage-Systeme werden für die SnapVault-Replizierung vorbereitet . . . 17
Sichern und Überprüfen Ihrer Datenbanken . . . 19
SnapManager Backup – Überblick . . . 19
Backup-Strategie definieren . . . 20
Erstellen eines Profils für Ihre Datenbank . . . 22
Sichern Ihrer Datenbank . . . 25
Datenbank-Backups werden überprüft . . . 26
Planung wiederkehrender Backups . . . 27
Weitere Schritte . . . 29
Installations- und Setup-Handbuch für UNIX® . . . 30
Produktübersicht . . . 30
SnapManager Highlights . . . 30
Architektur von SnapManager . . . 31
Implementierungs-Workflow . . . 33
Bereitstellung wird vorbereitet . . . 34
SnapManager Lizenzierung . . . 34
Unterstützte Konfigurationen . . . 35

Unterstützte Speichertypen . . . 35
UNIX Host-Anforderungen . . . 36
Datenbanken werden konfiguriert . . . 36
Konfigurieren der Zieldatenbank . . . 36
Erstellen eines Oracle-Datenbankbenutzers für die Zieldatenbank . . . 36
Erstellen der Repository-Datenbankinstanz . . . 37
Erstellen eines Oracle-Benutzers für die Repository-Datenbankinstanz . . . 37
Überprüfen der Oracle Listener-Konfiguration . . . 38
SnapManager wird installiert . . . 38
Einrichtung von SnapManager . . . 39
Starten des SnapManager-Servers . . . 39
Zugriff auf die SnapManager Benutzeroberfläche . . . 39
SnapManager-Repository wird konfiguriert . . . 40
Sichern und Überprüfen Ihrer Datenbanken . . . 41
SnapManager Backup – Überblick . . . 42
Backup-Strategie definieren . . . 42
Erstellen eines Profils für Ihre Datenbank . . . 44
Sichern Ihrer Datenbank . . . 47
Datenbank-Backups werden überprüft . . . 49
Planung wiederkehrender Backups . . . 49
Weitere Schritte . . . 51
Administrationshandbuch für UNIX® . . . 53
Produktübersicht . . . 53
SnapManager Highlights . . . 53
Backups mit Snapshot Kopien erstellen . . . 54
Warum sollten Sie Archiv Log-Dateien beschneiden . . . 54
Konsolidierung von Archivierungsprotokolldaten . . . 54
Vollständige oder teilweise Wiederherstellung von Datenbanken . . . 55
Überprüfen des Backup-Status . . . 55
Datenbank-Backup-Klone . . . 55
Verfolgen Sie die Details und erstellen Sie Berichte . . . 56
Repositories . . . 56
Welche Profile sind . . . 57
Die Status der SnapManager-Operation lauten . . . 58
Wie SnapManager die Sicherheit gewährleistet . . . 60
Online-Hilfe aufrufen und drucken . . . 61
Empfohlene allgemeine Datenbanklayouts und Speicherkonfigurationen . . . 61
Einschränkungen bei der Arbeit mit SnapManager . . . 74
Backups mit Snapshot Kopien erstellen . . . 81
Warum sollten Sie Archiv Log-Dateien beschneiden . . . 82
Konsolidierung von Archivierungsprotokolldaten . . . 82
Vollständige oder teilweise Wiederherstellung von Datenbanken . . . 82
Überprüfen des Backup-Status . . . 83
Datenbank-Backup-Klone . . . 83
Verfolgen Sie die Details und erstellen Sie Berichte . . . 84

Repositories . . . 84
Welche Profile sind . . . 85
Die Status der SnapManager-Operation lauten . . . 86
Wiederherstellbare und nicht wiederherstellbare Ereignisse . . . 87
Wie SnapManager die Sicherheit gewährleistet . . . 87
Online-Hilfe aufrufen und drucken . . . 89
Empfohlene allgemeine Datenbanklayouts und Speicherkonfigurationen . . . 89
Definieren des Datenbank-Home mit der oratab-Datei . . . 90
Anforderungen für die Verwendung von RAC-Datenbanken mit SnapManager . . . 90
Anforderungen für die Verwendung von ASM-Datenbanken mit SnapManager . . . 91
Unterstützte Partitionsgeräte . . . 92
Unterstützung für ASMLib . . . 93
Unterstützung für ASM-Datenbanken ohne ASMLib . . . 93
Anforderungen für die Verwendung von Datenbanken mit NFS und SnapManager . . . 99
Beispiel für Datenbank-Volume-Layouts . . . 100
Einschränkungen bei der Arbeit mit SnapManager . . . 102
SnapManager Limitierungen für Clustered Data ONTAP . . . 108
Einschränkungen in Bezug auf Oracle Database . . . 108
Einschränkungen beim Volume-Management . . . 109
Upgrade von SnapManager . . . 109
SnapManager wird vorbereitet . . . 110
Aktualisieren der SnapManager-Hosts . . . 110
Aufgaben nach dem Upgrade . . . 111
Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade . . . 113
SnapManager wird konfiguriert . . . 121
SnapManager-Konfigurationsparameter . . . 121
Konfiguration von SnapDrive für UNIX für eine aktiv/aktiv-Umgebung von Veritas SFRAC . . . 130
Konfiguration von SnapManager zur Unterstützung der Veritas SFRAC-Umgebung . . . 130
Sicherstellen, dass ASM importierte Festplatten erkennt . . . 131
Sicherheits- und Anmeldeinformationsmanagement . . . 132
Was ist die Benutzerauthentifizierung . . . 133
Die rollenbasierte Zugriffssteuerung . . . 134
Verschlüsselte Passwörter für benutzerdefinierte Skripts speichern . . . 139
Zugriffsberechtigung für das Repository . . . 139
Zugriff auf Profile wird autorisiert . . . 140
Anzeigen von Benutzeranmeldeinformationen . . . 140
Löschen von Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile . . . 141
Löschen von Anmeldeinformationen für einzelne Ressourcen . . . 142
Profilverwaltung für effiziente Backups . . . 143
Aufgaben im Zusammenhang mit Profilen . . . 143
Info zu Profilen und Authentifizierung . . . 143
Profile werden erstellt . . . 144
Benennen von Snapshot-Kopien . . . 151
Profile werden umbenannt . . . 153
Profilkennwörter werden geändert . . . 153

Profilkennwort wird zurückgesetzt . . . 154
Zugriff auf Profile wird autorisiert . . . 154
Profile werden überprüft . . . 154
Profile werden aktualisiert . . . 155
Profile werden gelöscht . . . 160
Backup von Datenbanken . . . 160
Welche SnapManager Datenbank-Backups sind . . . 162
Welche vollständigen und teilweisen Backups sind . . . 162
Über die Handhabung von Steuerdateien und Archivprotokolldateien . . . 168
Was ist für ein Datenbank-Backup geplant . . . 169
Datenbank-Backups werden erstellt . . . 173
Was ist AutoSupport . . . 187
Datenbank-Backups werden überprüft . . . 188
Ändern der Richtlinie zur Aufbewahrung von Backups . . . 189
Anzeigen einer Liste von Backups . . . 191
Anzeigen von Backup-Details . . . 191
Montage von Backups . . . 192
UnMounten von Backups . . . 193
So werden Backups entlastet . . . 194
Backups werden gelöscht . . . 195
Planen von Datenbank-Backups . . . 197
Erstellen von Backup-Zeitplänen . . . 197
Aktualisieren eines Backup-Zeitplans . . . 200
Anzeigen einer Liste geplanter Vorgänge . . . 201
Anhalten von Backup-Zeitplänen . . . 201
Wiederaufnahme der Backup-Pläne . . . 201
Löschen von Backup-Zeitplänen . . . 201
Datenbank-Backups werden wiederhergestellt . . . 201
Was ist Datenbank-Restore . . . 202
Anzeigen der Informationen zur Wiederherstellung von Backups in der Vorschau . . . 227
Wiederherstellung von Backups mit schneller Wiederherstellung . . . 229
Wiederherstellen von Backups mithilfe von Single File SnapRestore . . . 231
Wiederherstellung von Backups auf dem Primärspeicher . . . 231
Durchführen von Recovery auf Blockebene mit Oracle Recovery Manager (RMAN) . . . 236
Wiederherstellung von Dateien aus einem anderen Speicherort . . . 240
Klonen der Datenbank-Backup . . . 245
Klonen . . . 245
Klonmethoden . . . 247
Erstellen von Klonspezifikationen . . . 248
Klonen von Datenbanken aus Backups . . . 255
Das Klonen von Datenbanken im aktuellen Status . . . 256
Klonen von Datenbank-Backups ohne Umsetzungsprotokolle . . . 257
Überlegungen beim Klonen einer Datenbank auf einem alternativen Host . . . 258
Anzeigen einer Liste von Klonen . . . 259
Anzeigen detaillierter Kloninformationen . . . 260

Klone werden gelöscht . . . 260
Durch das Aufteilen eines Klons . . . 261
Einführung in Datensicherung in SnapManager . . . 264
Was sind Sicherungsrichtlinien . . . 265
Welche Schutzzustände sind . . . 266
Was sind Ressourcen-Pools . . . 267
Allgemeines zu unterschiedlichen Sicherungsrichtlinien . . . 267
Konfiguration und Aktivierung richtlinienbasierter Datensicherung . . . 269
Wie SnapManager Backups auf dem lokalen Storage aufbewahrt . . . 272
Überlegungen zur Durchführung der Datensicherung . . . 276
Sicherung von Datenbank-Backups auf sekundärem oder tertiärem Storage . . . 277
Wiederherstellen geschützter Backups aus dem sekundären Speicher . . . 279
Klonen geschützter Backups . . . 283
SnapManager für Oracle verwendet Protection Manager, um ein Datenbank-Backup zu schützen . . . 283
Details der Zieldatenbank . . . 284
Konfiguration und Topologie des primären und sekundären Storage . . . 284
Backup-Zeitplan und Aufbewahrungsstrategie . . . 288
Workflow-Zusammenfassung für lokale und sekundäre Datenbank-Backups . . . 289
Geschützte Backup-Konfiguration und -Ausführung . . . 290
Datenbankwiederherstellung aus Backup . . . 298
Durchführung von Managementvorgängen . . . 301
Anzeigen einer Liste von Vorgängen . . . 301
Anzeigen von Betriebsdetails . . . 301
Befehle von einem alternativen Host ausgeben . . . 302
Überprüfen der SnapManager-Softwareversion . . . 302
Beenden des SnapManager-Hostservers . . . 302
Starten Sie den SnapManager UNIX-Hostserver neu . . . 302
Deinstallieren der Software von einem UNIX-Host . . . 303
Konfigurieren einer E-Mail-Benachrichtigung . . . 303
Konfigurieren eines E-Mail-Servers für ein Repository . . . 304
Konfigurieren der E-Mail-Benachrichtigung für ein neues Profil . . . 306
Konfigurieren der E-Mail-Benachrichtigung für ein vorhandenes Profil . . . 308
Konfigurieren einer E-Mail-Benachrichtigung mit Zusammenfassung für mehrere Profile . . . 309
Hinzufügen eines neuen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung . . . 310
Hinzufügen eines vorhandenen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung . . . 310
Deaktivieren der E-Mail-Benachrichtigung für mehrere Profile . . . 310
Erstellen von Aufgabenspezifikationsdatei und Skripten für SnapManager-Vorgänge . . . 311
Erstellen von vor-, Post-Task- und Richtlinienskripten . . . 313
Anzeigen von Beispielskripten für das Plug-in . . . 325
Aufgabenskripte werden erstellt . . . 328
Speichern der Taskskripte . . . 329
Überprüfen der Installation von Plug-in-Skripten . . . 330
Erstellen einer Aufgabenspezifikationsdatei . . . 331
Durchführung von Backup-, Restore- und Klonvorgängen mithilfe von Prescript und Post-Scripts . . . 333
Der Name des Speichersystems und der dem Profil zugeordneten Zieldatenbank-Hostname werden

aktualisiert . . . 335
Der Name des Speichersystems, der einem Profil zugeordnet ist, wird aktualisiert . . . 335
Anzeigen einer Liste von Speichersystemen, die einem Profil zugeordnet sind . . . 336
Der Host-Name der Zieldatenbank, der einem Profil zugeordnet ist, wird aktualisiert . . . 337
Historie von SnapManager-Vorgängen aufrechterhalten . . . 338
Konfigurieren des Verlaufs für den SnapManager-Vorgang . . . 339
Anzeigen einer Liste des SnapManager-Betriebsverlaufs . . . 339
Anzeigen des detaillierten Verlaufs einer bestimmten Operation, die einem Profil zugeordnet ist . . . 340
Löschen des Verlaufs des SnapManager-Vorgangs . . . 340
Entfernen von Verlaufseinstellungen, die einem einzelnen Profil oder mehreren Profilen zugeordnet sind . . . 340
Anzeigen der Konfigurationsdetails des SnapManager-Verlaufs . . . 340
Befehlsreferenz für SnapManager für Oracle . . . 341
Der Befehl smo_Server restart . . . 341
Der Befehl smo_Server Start . . . 342
Der Status-Befehl smo_Server . . . 342
Der Befehl smo_Server stop . . . 343
Der Befehl smo Backup erstellen . . . 344
Der Befehl smo Backup delete . . . 348
Der smo Backup kostenlose Befehl . . . 350
Der Befehl smo Backup list . . . 351
Der Befehl smo Backup Mount . . . 352
Der Smo Backup Restore Befehl . . . 355
Der Befehl smo Backup show . . . 359
Der Befehl smo Backup unmount . . . 362
Der SMO-Befehl zum Aktualisieren der Datensicherung . . . 363
Der Befehl smo Backup verify . . . 365
Der Befehl Smo Clone create . . . 366
Der Befehl smo Clone delete . . . 370
Der Befehl smo Clone list . . . 372
Der Befehl smo Clone show . . . 373
Der Befehl smo Clone template . . . 376
Der Befehl smo Clone Update . . . 377
Der Befehl smo Clone Split-delete . . . 378
Der Befehl smo Clone Split-Schätzen . . . 379
Der Befehl smo Clone Split . . . 380
Der Befehl smo Clone Split-Ergebnis . . . 386
Der Befehl smo Clone Split-stop . . . 387
Der Befehl smo Clone Split-Status . . . 387
Der Befehl Smo Clone Trennen . . . 388
Der Befehl smo cmdfile . . . 389
Der Befehl smo Credential Clear . . . 390
Der Befehl zum Löschen von Smo-Anmeldeinformationen . . . 391
Der Befehl smo Anmeldeinformationsliste . . . 393
Der Befehl Smo Credential Set . . . 394

Der Befehl smo history list . . . 396
Der Befehl smo history Operation-show . . . 397
Der Befehl Smo history purge . . . 398
Der Befehl smo history remove . . . 399
Der Befehl smo history set . . . 401
Der Befehl smo history show . . . 403
Der Befehl smo help . . . 403
Der Befehl smo notification remove-summary-notification . . . 404
Der Befehl smo notification Update-summary-notification . . . 405
Der Befehl smo notification set . . . 407
Der Befehl Smo Operation Dump . . . 409
Befehl smo Operation list . . . 410
Der Befehl smo Operation show . . . 411
Der Befehl smo password Reset . . . 413
Der smo Plugin Check Befehl . . . 414
Der Befehl smo profile create . . . 415
Der Befehl smoprofile delete . . . 421
Der Befehl smo profile destroy . . . 422
Der Befehl smoprofile dump . . . 423
Der Befehl smo profile list . . . 423
Der Befehl smo profile show . . . 425
Der Befehl smo profile SYNC . . . 426
Der Befehl smoprofile Update . . . 428
Der Befehl smoprofile verify . . . 434
Der Befehl smo Protection-Policy . . . 435
Der Befehl smo Repository create . . . 436
Der Befehl smo Repository löschen . . . 438
Der smo Repository Rollback-Befehl . . . 440
Der Befehl smo Repository Rolling Upgrade . . . 442
Der Befehl smo Repository show . . . 443
Der Befehl smo Repository Update . . . 445
Der Befehl smo schedule create . . . 446
Der Befehl smo schedule delete . . . 451
Der Befehl smo schedule list . . . 451
Der Smo Schedule Resume Befehl . . . 452
Der Befehl smoplan suspendieren . . . 452
Der Befehl smo schedule Update . . . 453
Der Befehl smo Storage list . . . 454
Der Befehl smo Storage umbenennen . . . 455
Der SMO System Dump Befehl . . . 456
Der Befehl smo System verify . . . 456
Der Befehl smo Version . . . 457
SnapManager zur Fehlerbehebung . . . 458
Speicherauszug-Dateien . . . 464
Fehlerbehebung bei Klonproblemen . . . 470

Fehlerbehebung bei Problemen mit der grafischen Benutzeroberfläche . . . 473
Fehlerbehebung bei SnapDrive-Problemen . . . 479
Fehlerbehebung bei der Umbenennung des Speichersystems . . . 481
Fehlerbehebung bei bekannten Problemen . . . 482
Montage eines FlexClone Volume schlägt in der NFS-Umgebung fehl . . . 488
Ausführung mehrerer paralleler Vorgänge schlägt in SnapManager fehl . . . 488
RAC-Datenbank kann von einem der RAC-Knoten, in dem das Profil nicht erstellt wurde, nicht wiederhergestellt werden . . . 489
Weitere Informationen . . . 489
Klassifizierungen für Fehlermeldungen . . . 490
Fehlermeldungen . . . 492
Die häufigsten Fehlermeldungen . . . 492
Fehlermeldungen im Zusammenhang mit dem Datenbank-Backup-Prozess (Serie 2000) . . . 500
Datensicherungsfehler . . . 501
Fehlermeldungen im Zusammenhang mit dem Wiederherstellungsprozess (Serie 3000) . . . 505
Fehlermeldungen, die mit dem Klonprozess verbunden sind (4000 Serie) . . . 508
Fehlermeldungen im Zusammenhang mit der Verwaltung des Profilprozesses (5000-Serie) . . . 509
Fehlermeldungen im Zusammenhang mit der Entlastung von Backup-Ressourcen (Backups 6000 Serie) . . . 509
Fehler bei der virtuellen Storage-Schnittstelle (Virtual Storage Interface 8000 Serie) . . . 510
Fehlermeldungen zum Rolling Upgrade-Prozess (Serie 9000) . . . 510
Ausführung von Operationen (12,000 Serie) . . . 512
Ausführung von Prozesskomponenten (Serie 13,000) . . . 512
Fehlermeldungen zu SnapManager Utilities (14,000 Series) . . . 513
Allgemeine Fehlermeldungen bei SnapDrive für UNIX . . . 515
Installations- und Administrationsanleitung . . . 517
Was ist SnapManagerfür Oracle . . . 517
Was macht SnapManager für Oracle . . . 517
Integration in andere Applikationen und Technologien von NetApp . . . 520
Vorteile von SnapManager . . . 521
Die Architektur von SnapManager für Oracle ist das . . . 524
Repositories . . . 526
Welche Profile sind . . . 527
Die Status der SnapManager-Operation lauten . . . 528
Wie SnapManager die Sicherheit gewährleistet . . . 529
Online-Hilfe aufrufen und drucken . . . 530
Überlegungen zur Implementierung von SnapManager für Oracle . . . 531
Anforderungen für die Ausführung von SnapManager . . . 531
Versionsunterstützung und Übersicht über die Konfiguration der Datenbank . . . 533
Einschränkungen bei der Arbeit mit SnapManager . . . 534
SnapManager Funktionen und Oracle Technologien, die unter Windows nicht unterstützt werden . . . 538
SnapManager Limitierungen für Clustered Data ONTAP . . . 539
Einschränkungen in Bezug auf Oracle Database . . . 539
Veraltete Versionen der Oracle-Datenbank . . . 540
Installation von SnapManager für Oracle . . . 540

Installation von SnapManager für Oracle wird vorbereitet . . . 540
Installation von SnapManager für Oracle . . . 542
Upgrade von SnapManager . . . 543
SnapManager wird vorbereitet . . . 543
Aktualisieren von SnapManager-Hosts . . . 544
Aufgaben nach dem Upgrade . . . 545
Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade . . . 547
SnapManager wird konfiguriert . . . 554
SnapManager-Konfigurationsparameter . . . 554
Starten von SnapManagerfür Oracle . . . 562
Identifizieren einer vorhandenen Datenbank für das Backup . . . 563
Überprüfen des Oracle Listener-Status . . . 563
Erstellen von Oracle-Benutzern für die Repository-Datenbank . . . 563
Erstellen eines Oracle-Benutzers für die Zieldatenbank . . . 564
Zugriff auf SnapManager . . . 564
Überprüfen der Umgebung . . . 567
Repositories werden erstellt . . . 568
Reihenfolge der Durchführung von Vorgängen . . . 571
Sicherheits- und Anmeldeinformationsmanagement . . . 572
Was ist die Benutzerauthentifizierung . . . 572
Verschlüsselte Passwörter für benutzerdefinierte Skripts speichern . . . 573
Zugriffsberechtigung für das Repository . . . 574
Zugriff auf Profile wird autorisiert . . . 574
Anzeigen von Benutzeranmeldeinformationen . . . 574
Löschen von Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile . . . 575
Löschen von Anmeldeinformationen für einzelne Ressourcen . . . 576
Profilverwaltung für effiziente Backups . . . 577
Aufgaben im Zusammenhang mit Profilen . . . 577
Info zu Profilen und Authentifizierung . . . 577
Profile werden erstellt . . . 578
Benennen von Snapshot-Kopien . . . 582
Profile werden umbenannt . . . 584
Profilkennwörter werden geändert . . . 585
Profilkennwort wird zurückgesetzt . . . 585
Zugriff auf Profile wird autorisiert . . . 586
Profile werden überprüft . . . 586
Profile werden aktualisiert . . . 586
Profile werden gelöscht . . . 590
Backup von Datenbanken . . . 590
Welche SnapManager Datenbank-Backups sind . . . 591
Welche vollständigen und teilweisen Backups sind . . . 592
Über die Handhabung von Steuerdateien und Archivprotokolldateien . . . 598
Was ist für ein Datenbank-Backup geplant . . . 599
Datenbank-Backups werden erstellt . . . 603
Was ist AutoSupport . . . 616

Datenbank-Backups werden überprüft . . . 617
Ändern der Richtlinie zur Aufbewahrung von Backups . . . 618
Anzeigen einer Liste von Backups . . . 620
Anzeigen von Backup-Details . . . 620
Montage von Backups . . . 621
UnMounten von Backups . . . 622
So werden Backups entlastet . . . 622
Backups werden gelöscht . . . 622
Planen von Datenbank-Backups . . . 623
Erstellen von Backup-Zeitplänen . . . 623
Aktualisieren eines Backup-Zeitplans . . . 626
Anzeigen einer Liste geplanter Vorgänge . . . 627
Anhalten von Backup-Zeitplänen . . . 627
Wiederaufnahme der Backup-Pläne . . . 627
Löschen von Backup-Zeitplänen . . . 627
Datenbank-Backups werden wiederhergestellt . . . 627
Was ist Datenbank-Restore . . . 628
Anzeigen der Informationen zur Wiederherstellung von Backups in der Vorschau . . . 632
Wiederherstellung von Backups auf dem Primärspeicher . . . 633
Durchführen von Recovery auf Blockebene mit Oracle Recovery Manager (RMAN) . . . 637
Wiederherstellung von Dateien aus einem anderen Speicherort . . . 641
Klonen der Datenbank-Backup . . . 644
Klonen . . . 644
Klonmethoden . . . 646
Erstellen von Klonspezifikationen . . . 646
Klonen von Datenbanken aus Backups . . . 653
Das Klonen von Datenbanken im aktuellen Status . . . 655
Klonen von Datenbank-Backups ohne Umsetzungsprotokolle . . . 655
Überlegungen beim Klonen einer Datenbank auf einem alternativen Host . . . 656
Anzeigen einer Liste von Klonen . . . 657
Anzeigen detaillierter Kloninformationen . . . 658
Klone werden gelöscht . . . 658
Einführung in Datensicherung in SnapManager . . . 659
Wie SnapManager Backups auf dem lokalen Storage aufbewahrt . . . 659
Überlegungen zur Durchführung der Datensicherung . . . 662
Sicherung von Datenbank-Backups mithilfe von Postskripten . . . 663
Durchführung von Managementvorgängen . . . 676
Anzeigen einer Liste von Vorgängen . . . 676
Anzeigen von Betriebsdetails . . . 677
Befehle von einem alternativen Host ausgeben . . . 677
Überprüfen der SnapManager-Softwareversion . . . 678
Beenden des SnapManager-Hostservers . . . 678
Starten Sie den SnapManager-Hostserver neu . . . 678
Deinstallieren von SnapManager . . . 678
Konfigurieren einer E-Mail-Benachrichtigung . . . 679

Konfigurieren eines E-Mail-Servers für ein Repository . . . 680
Konfigurieren der E-Mail-Benachrichtigung für ein neues Profil . . . 681
Konfigurieren der E-Mail-Benachrichtigung für ein vorhandenes Profil . . . 683
Konfigurieren einer E-Mail-Benachrichtigung mit Zusammenfassung für mehrere Profile . . . 684
Hinzufügen eines neuen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung . . . 685
Hinzufügen eines vorhandenen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung . . . 685
Deaktivieren der E-Mail-Benachrichtigung für mehrere Profile . . . 685
Erstellen von Aufgabenspezifikationsdatei und Skripten für SnapManager-Vorgänge . . . 686
Erstellen von vor-, Post-Task- und Richtlinienskripten . . . 688
Anzeigen von Beispielskripten für das Plug-in . . . 699
Aufgabenskripte werden erstellt . . . 702
Speichern der Taskskripte . . . 703
Überprüfen der Installation von Plug-in-Skripten . . . 704
Erstellen einer Aufgabenspezifikationsdatei . . . 705
Durchführung von Backup-, Restore- und Klonvorgängen mithilfe von Prescript und Post-Scripts . . . 707
Der Name des Speichersystems und der dem Profil zugeordneten Zieldatenbank-Hostname werden aktualisiert . . . 709
Der Name des Speichersystems, der einem Profil zugeordnet ist, wird aktualisiert . . . 709
Anzeigen einer Liste von Speichersystemen, die einem Profil zugeordnet sind . . . 710
Der Host-Name der Zieldatenbank, der einem Profil zugeordnet ist, wird aktualisiert . . . 710
Historie von SnapManager-Vorgängen aufrechterhalten . . . 711
Konfigurieren des Verlaufs für den SnapManager-Vorgang . . . 712
Anzeigen einer Liste des SnapManager-Betriebsverlaufs . . . 713
Anzeigen des detaillierten Verlaufs einer bestimmten Operation, die einem Profil zugeordnet ist . . . 713
Löschen des Verlaufs des SnapManager-Vorgangs . . . 713
Entfernen von Verlaufseinstellungen, die einem einzelnen Profil oder mehreren Profilen zugeordnet sind . . . 713
Anzeigen der Konfigurationsdetails des SnapManager-Verlaufs . . . 714
Befehlsreferenz für SnapManager für Oracle . . . 714
Der Befehl smo_Server restart . . . 714
Der Befehl smo_Server Start . . . 715
Der Status-Befehl smo_Server . . . 716
Der Befehl smo_Server stop . . . 716
Der Befehl smo Backup erstellen . . . 717
Der Befehl smo Backup delete . . . 721
Der smo Backup kostenlose Befehl . . . 723
Der Befehl smo Backup list . . . 724
Der Befehl smo Backup Mount . . . 725
Der Smo Backup Restore Befehl . . . 727
Der Befehl smo Backup show . . . 731
Der Befehl smo Backup unmount . . . 732
Der SMO-Befehl zum Aktualisieren der Datensicherung . . . 734
Der Befehl smo Backup verify . . . 736
Der Befehl Smo Clone create . . . 737
Der Befehl smo Clone delete . . . 740

Der Befehl smo Clone list . . . 742
Der Befehl smo Clone show . . . 743
Der Befehl smo Clone template . . . 745
Der Befehl smo Clone Update . . . 746
Der Befehl Smo Clone Trennen . . . 747
Der Befehl smo cmdfile . . . 747
Der Befehl smo Credential Clear . . . 748
Der Befehl zum Löschen von Smo-Anmeldeinformationen . . . 749
Der Befehl smo Anmeldeinformationsliste . . . 751
Der Befehl Smo Credential Set . . . 752
Der Befehl smo history list . . . 754
Der Befehl smo history Operation-show . . . 755
Der Befehl Smo history purge . . . 756
Der Befehl smo history remove . . . 757
Der Befehl smo history set . . . 759
Der Befehl smo history show . . . 761
Der Befehl smo help . . . 761
Der Befehl smo notification remove-summary-notification . . . 762
Der Befehl smo notification Update-summary-notification . . . 763
Der Befehl smo notification set . . . 765
Der Befehl Smo Operation Dump . . . 767
Befehl smo Operation list . . . 768
Der Befehl smo Operation show . . . 769
Der Befehl smo password Reset . . . 771
Der Befehl smo profile create . . . 772
Der Befehl smoprofile delete . . . 777
Der Befehl smoprofile dump . . . 778
Der Befehl smo profile list . . . 778
Der Befehl smo profile show . . . 780
Der Befehl smo profile SYNC . . . 781
Der Befehl smoprofile Update . . . 782
Der Befehl smoprofile verify . . . 787
Der Befehl smo Repository create . . . 789
Der Befehl smo Repository löschen . . . 791
Der smo Repository Rollback-Befehl . . . 793
Der Befehl smo Repository rollingupgrade . . . 795
Der Befehl smo Repository show . . . 796
Der Befehl smo Repository Update . . . 798
Der Befehl smo schedule create . . . 799
Der Befehl smo schedule delete . . . 804
Der Befehl smo schedule list . . . 804
Der Smo Schedule Resume Befehl . . . 804
Der Befehl smoplan suspendieren . . . 805
Der Befehl smo schedule Update . . . 805
Der Befehl smo Storage list . . . 807

Der Befehl smo Storage umbenennen . . . 807
Der SMO System Dump Befehl . . . 808
Der Befehl smo System verify . . . 809
Der Befehl smo Version . . . 810
SnapManager zur Fehlerbehebung . . . 810
Speicherauszug-Dateien . . . 819
Fehlerbehebung bei Klonproblemen . . . 824
Fehlerbehebung bei Problemen mit der grafischen Benutzeroberfläche . . . 826
Fehlerbehebung bei bekannten Problemen . . . 832
Ausführung mehrerer paralleler Vorgänge schlägt in SnapManager fehl . . . 835
RAC-Datenbank kann von einem der RAC-Knoten, in dem das Profil nicht erstellt wurde, nicht wiederhergestellt werden . . . 835
Weitere Informationen . . . 836
Klassifizierungen für Fehlermeldungen . . . 837
Fehlermeldungen . . . 839
Die häufigsten Fehlermeldungen . . . 839
Fehlermeldungen im Zusammenhang mit dem Datenbank-Backup-Prozess (Serie 2000) . . . 844
Fehlermeldungen im Zusammenhang mit dem Wiederherstellungsprozess (Serie 3000) . . . 845
Fehlermeldungen, die mit dem Klonprozess verbunden sind (4000 Serie) . . . 847
Fehlermeldungen im Zusammenhang mit der Verwaltung des Profilprozesses (5000-Serie) . . . 848
Fehlermeldungen im Zusammenhang mit der Entlastung von Backup-Ressourcen (Backups 6000 Serie) . . . 848
Fehlermeldungen zum Rolling Upgrade-Prozess (Serie 9000) . . . 849
Ausführung von Operationen (12,000 Serie) . . . 850
Ausführung von Prozesskomponenten (Serie 13,000) . . . 850
Fehlermeldungen zu SnapManager Utilities (14,000 Series) . . . 851
Rechtliche Hinweise . . . 854
Urheberrecht . . . 854
Marken . . . 854
Patente . . . 854
Datenschutzrichtlinie . . . 854
Open Source . . . 854

SnapManager 3.4.2 für Oracle

Willkommen bei der SnapManager for Oracle Information Library. Hier finden Sie Informationen zu SnapManager 3.4.2 für Oracle, einschließlich Einrichtung, Management und Konfiguration der Software für Clustered Data ONTAP sowie für Data ONTAP in 7-Mode.

Versionshinweise zu SnapManager 3.4.2 für Oracle

Der "Versionshinweise zu SnapManager 3.4.2 für Oracle" Beschreiben Sie neue Funktionen, Upgrade-Hinweise, feste Probleme, bekannte Einschränkungen und bekannte Probleme.

Sie müssen sich auf der NetApp Support-Website anmelden, um auf die Versionshinweise zuzugreifen.

Installations- und Setup-Handbuch für UNIX®

In diesem Leitfaden werden die ersten Aufgaben beschrieben, die für die Bereitstellung von SnapManager 3.4.2 für Oracle mit Clustered Data ONTAP in einer UNIX Umgebung erforderlich sind. Die Themen umfassen die Installation und Konfiguration des Produkts sowie die Sicherung der Datenbanken.

Produktübersicht

SnapManager für Oracle automatisiert und vereinfacht komplexe, manuelle und zeitintensive Prozesse, die im Zusammenhang mit Backup, Recovery und Klonen von Oracle Datenbanken anfallen. Mithilfe von SnapManager mit Data ONTAP SnapMirror Technologie können Sie Backup-Kopien auf einem anderen Volume erstellen. Mit der Data ONTAP SnapVault Technologie werden Backups effizient auf Festplatten archiviert.

SnapManager lässt sich mit nativen Oracle Technologien wie Oracle Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) und Direct NFS über FC-, iSCSI- und NFS-Protokolle integrieren. Optional können mit SnapManager erstellte Backups mit dem Oracle Recovery Manager (RMAN) katalogisiert werden, um die Backup-Informationen zu erhalten. Diese Backups können später in Restore-Vorgängen auf Blockebene oder in zeitpunktgenauen Recovery-Vorgängen verwendet werden.

SnapManager Highlights

SnapManager ermöglicht die nahtlose Integration mit Oracle Datenbanken auf dem UNIX Host und über das Backend mit NetApp Snapshot, SnapRestore und FlexClone Technologien Es bietet eine benutzerfreundliche Oberfläche (UI) und eine Befehlszeilenschnittstelle (CLI) für Administrationsfunktionen.

Mit SnapManager können Sie folgende Datenbankvorgänge ausführen und Daten effizient managen:

- Erstellung platzsparender Backups auf primärem oder sekundärem Storage

  SnapManager ermöglicht Ihnen ein separates Backup der Datendateien und die Archivierung von Protokolldateien.

- Planen von Backups
- Wiederherstellung vollständiger oder partieller Datenbanken unter Verwendung eines dateibasierten oder Volume-basierten Restore-Vorgangs
- Wiederherstellung von Datenbanken durch Erkennung, Mounten und Anwendung von Archivprotokolldateien aus Backups
- Beschneiden von Archiv-Log-Dateien von Archiv-Protokollzielen bei der Erstellung von Backups nur der Archivprotokolle
- Automatische Aufbewahrung einer minimalen Anzahl von Archiv-Log-Backups, da nur die Backups gespeichert werden, die eindeutige Archivprotokolldateien enthalten
- Verfolgung von Betriebsdetails und Erstellung von Berichten
- Backup wird überprüft, um sicherzustellen, dass sich Backups in einem gültigen Blockformat befinden und dass keine der gesicherten Dateien beschädigt sind
- Pflegen eines Verlaufs von Vorgängen, die im Datenbankprofil durchgeführt werden

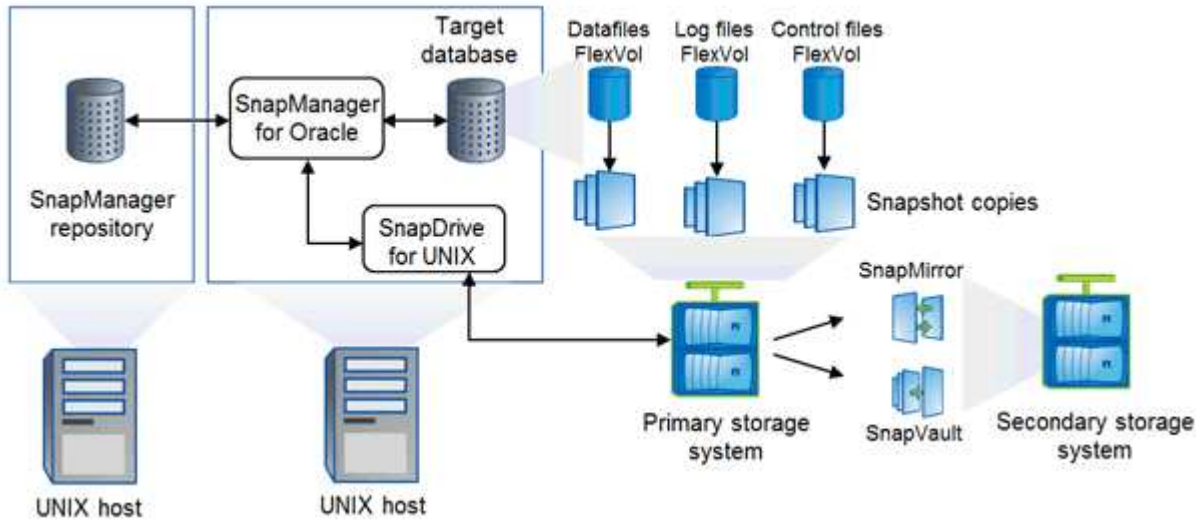
Ein Profil enthält Informationen über die Datenbank, die von SnapManager gemanagt werden soll.

- Sicherung von Backups auf sekundären Storage-Systemen.
- Erstellung platzsparender Backup-Klone auf primärem oder sekundärem Storage

  SnapManager ermöglicht Ihnen die Aufteilung eines Datenbankklonen.

Architektur von SnapManager

SnapManager für Oracle enthält Komponenten, die gemeinsam eine umfassende und leistungsstarke Backup-, Restore-, Recovery- und Klonlösung für Oracle Datenbanken bieten.



SnapDrive für UNIX

SnapManager benötigt SnapDrive, um die Verbindung zum Storage-System herzustellen. Sie müssen SnapDrive for UNIX auf jedem Ziel-Datenbank-Host installieren, bevor Sie SnapManager installieren.

SnapManager für Oracle

Sie müssen SnapManager für Oracle auf jedem Ziel-Datenbank-Host installieren.

Sie können entweder die Befehlszeilenschnittstelle (CLI) oder die Benutzeroberfläche vom Datenbank-Host verwenden, auf dem SnapManager für Oracle installiert ist. Sie können die SnapManager-Benutzeroberfläche auch Remote verwenden, indem Sie einen Webbrowser von jedem System verwenden, das auf einem von SnapManager unterstützten Betriebssystem ausgeführt wird.

Die unterstützten JRE-Versionen sind 1.5, 1.6, 1.7 und 1.8.

Zieldatenbank

Die Zieldatenbank ist eine Oracle Datenbank, die Sie mit SnapManager managen möchten, indem Sie Backup-, Restore-, Recovery- und Klonvorgänge durchführen.

Die Zieldatenbank kann eine eigenständige Real Application Clusters (RAC) sein oder auf Oracle Automatic Storage Management (ASM)-Volumes residieren. Weitere Informationen zu den unterstützten Oracle

Datenbankversionen, Konfigurationen, Betriebssystemen und Protokollen finden Sie im NetApp Interoperabilitäts-Matrix-Tool.

SnapManager Repository

Das SnapManager Repository befindet sich in einer Oracle Datenbank und speichert Metadaten zu Profilen, Backups, Restores, Recoverys und Klonen. Ein einziges Repository kann Informationen über Vorgänge enthalten, die an mehreren Datenbankprofilen durchgeführt werden.

Das SnapManager-Repository kann sich nicht in der Zieldatenbank befinden. Die SnapManager-Repository-Datenbank und die Zieldatenbank müssen online sein, bevor SnapManager Vorgänge durchgeführt werden können.

Primärspeicher

SnapManager sichert die Zieldatenbanken auf dem primären NetApp Storage-System.

Sekundäres Storage-System

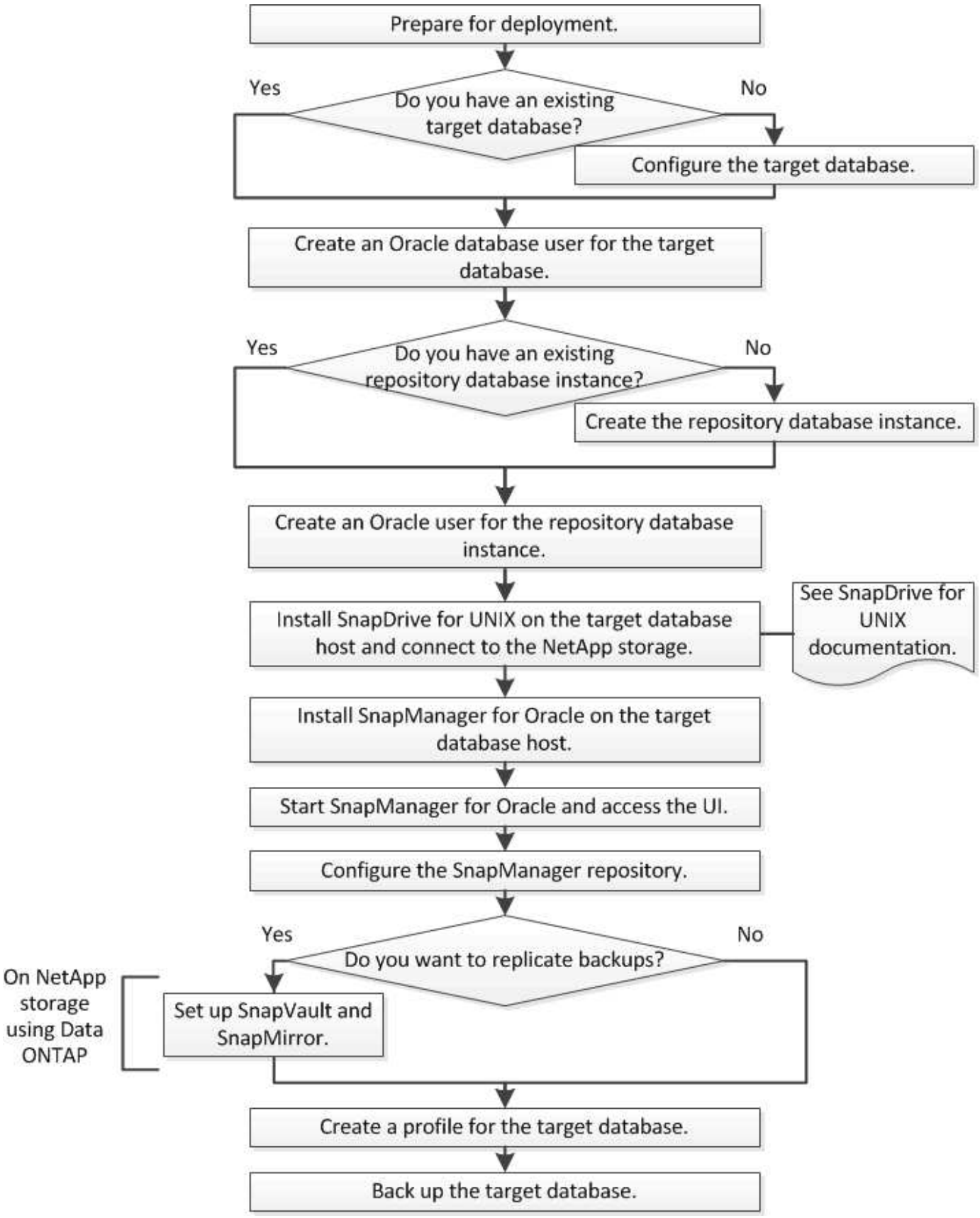
Wenn Sie die Datensicherung in einem Datenbankprofil ermöglichen, werden die Backups, die von SnapManager auf dem primären Storage-System erstellt wurden, mithilfe von SnapVault und SnapMirror Technologien auf ein sekundäres NetApp Storage-System repliziert.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Implementierungs-Workflow

Bevor Sie Backups mit SnapManager erstellen können, müssen Sie zuerst SnapDrive für UNIX installieren und dann SnapManager für Oracle installieren.



Bereitstellung wird vorbereitet

Bevor Sie SnapManager bereitstellen, müssen Sie sicherstellen, dass Ihr

Speichersystem und UNIX-Hosts die Mindestanforderungen für die Ressourcen erfüllen.

1. Stellen Sie sicher, dass Sie über die erforderlichen Lizenzen verfügen.
2. Überprüfen Sie die unterstützten Konfigurationen.
3. Überprüfen Sie die unterstützten Speichertypen.
4. Vergewissern Sie sich, dass Ihre UNIX Hosts die SnapManager-Anforderungen erfüllen.

SnapManager Lizenzierung

Zur Aktivierung des SnapManager Betriebs sind eine SnapManager Lizenz und mehrere Storage-System-Lizenzen erforderlich. Die SnapManager Lizenz ist in zwei Lizenzmodellen erhältlich: Lizenzierung pro Server. Bei diesem Modell befindet sich die SnapManager Lizenz auf jedem Datenbank-Host und die Lizenzierung erfolgt pro Storage-System. In diesem Modell befindet sich die SnapManager Lizenz im Storage-System.

Die SnapManager Lizenzanforderungen lauten wie folgt:

Lizenz	Beschreibung	Bei Bedarf
SnapManager pro Server	Eine Host-seitige Lizenz für einen bestimmten Datenbank-Host. Die Lizenzen sind nur für Datenbank-Hosts erforderlich, auf denen SnapManager installiert ist. Für das Storage-System ist keine SnapManager Lizenz erforderlich.	Auf dem SnapManager-Host. Auf primären und sekundären Storage-Systemen ist keine SnapManager-Lizenz erforderlich, wenn die Lizenzierung pro Server verwendet wird.
SnapManager pro Storage-System	Eine Storage-seitige Lizenz, die eine beliebige Anzahl von Datenbank-Hosts unterstützt. Nur erforderlich, wenn Sie keine Serverlizenz auf dem Datenbank-Host verwenden.	Auf primären und sekundären Storage-Systemen.
SnapRestore	Eine erforderliche Lizenz zum Wiederherstellen von Datenbanken durch SnapManager.	Auf primären und sekundären Storage-Systemen.erforderlich auf SnapMirror Zielsystemen zur Remote-Verifizierung Erforderlich auf SnapVault Zielsystemen, um eine Remote-Verifizierung und die Wiederherstellung aus einem Backup durchzuführen.

Lizenz	Beschreibung	Bei Bedarf
FlexClone	Eine optionale Lizenz zum Klonen von Datenbanken.	Auf primären und sekundären Storage-Systemen.erforderlich auf SnapVault Zielsystemen beim Erstellen von Klonen aus einem Backup.
SnapMirror	Eine optionale Lizenz zum Spiegeln von Backups auf ein Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
SnapVault	Eine optionale Lizenz zur Archivierung von Backups auf einem Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
Protokolle	NFS-, iSCSI- oder FC-Lizenzen sind abhängig vom verwendeten Protokoll erforderlich.	Auf primären und sekundären Storage-Systemen. Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.

Unterstützte Konfigurationen

Die Hosts, auf denen Sie SnapManager installieren, müssen die angegebenen Software-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Vor der Installation oder dem Upgrade von SnapManager müssen Sie die Unterstützung Ihrer Konfiguration überprüfen.

Informationen zu unterstützten Konfigurationen finden Sie im Interoperabilitäts-Matrix-Tool.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Unterstützte Speichertypen

SnapManager unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf Virtual Machines. Sie müssen die Unterstützung Ihres Storage-Typs überprüfen, bevor Sie SnapManager installieren oder aktualisieren.

Maschine	Storage-Typ
Physischer Server	• Volumes mit NFS-Anbindung • FC-verbundene LUNs • ISCSI-verbundene LUNs

Maschine	Storage-Typ
VMware ESX	• NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • RDM-LUNs auf dem Gastbetriebssystem

UNIX Host-Anforderungen

Sie müssen SnapManager für Oracle auf jedem Host installieren, auf dem eine Oracle Datenbank, die Sie sichern möchten, gehostet wird. Sie müssen sicherstellen, dass Ihre Hosts die Mindestanforderungen für die SnapManager-Konfiguration erfüllen.

- Sie müssen SnapDrive auf dem Datenbank-Host installieren, bevor Sie SnapManager installieren.
- Sie können SnapManager entweder auf physischen oder virtuellen Maschinen installieren.
- Sie müssen dieselbe SnapManager-Version auf allen Hosts installieren, die sich dasselbe Repository teilen.
- Wenn Sie Oracle Databases 11.2.0.2 oder 11.2.0.3 verwenden, müssen Sie Oracle Patch 13366202 installieren.

  Wenn Sie DNFS verwenden, müssen Sie die Patches, die im My Oracle Support (MOS)-Bericht 1495104.1 aufgeführt sind, installieren, um maximale Performance und Stabilität zu erzielen.

Datenbanken werden konfiguriert

Sie müssen mindestens zwei Oracle Datenbanken konfigurieren: Eine Zieldatenbank, die Sie mit SnapManager sichern möchten, und eine Repository-Datenbank zum Speichern der Metadaten der Zieldatenbank. Die Zieldatenbank und die SnapManager Repository-Datenbank müssen konfiguriert und online sein, bevor SnapManager Vorgänge durchgeführt werden können.

Konfigurieren der Zieldatenbank

Die Zieldatenbank ist eine Oracle-Datenbank, die entweder als Standalone, Real Application Clusters (RAC), Automatic Storage Management (ASM) oder als andere unterstützte Kombinationen konfiguriert werden kann.

1. Konfigurieren Sie die Zieldatenbank, indem Sie auf *TR-3633* verweisen.

Verwandte Informationen

"NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage"

Erstellen eines Oracle-Datenbankbenutzers für die Zieldatenbank

Ein Benutzer der Oracle-Datenbank muss sich bei der Datenbank anmelden und SnapManager Vorgänge durchführen. Sie müssen diesen Benutzer mit der Berechtigung *sysdba* erstellen, wenn für die Zieldatenbank kein Benutzer mit der Berechtigung *sysdba*

vorhanden ist.

SnapManager kann jeden Oracle-Benutzer mit der Berechtigung *sysdba* verwenden, die für die Zieldatenbank vorhanden ist. Beispielsweise kann SnapManager den standardmäßigen Benutzer *sys* verwenden. Selbst wenn der Benutzer vorhanden ist, können Sie jedoch einen neuen Benutzer für die Zieldatenbank erstellen und die Berechtigung *sysdba* zuweisen.

Sie können auch die OS-Authentifizierungsmethode verwenden, bei der das Betriebssystem (OS) es der Oracle-Datenbank ermöglicht, die vom Betriebssystem gepflegten Anmeldeinformationen zu verwenden, um Benutzer zur Anmeldung in der Datenbank und zur Durchführung von SnapManager-Vorgängen zu authentifizieren. Wenn Sie über das Betriebssystem authentifiziert sind, können Sie eine Verbindung zur Oracle-Datenbank herstellen, ohne einen Benutzernamen oder ein Kennwort anzugeben.

1. Melden Sie sich bei SQL an *Plus: Sqlplus '/ AS sysdba'
2. Erstellen Sie einen neuen Benutzer mit einem Administrator-Passwort: Erstellen Sie useruser_Name, der durch admin_password identifiziert wurde;

   User_Name ist der Name des Benutzers, den Sie erstellen, und admin_password ist das Passwort, das Sie dem Benutzer zuweisen möchten.

3. Weisen Sie dem neuen Oracle-Benutzer die sysdba-Berechtigung zu: Erteilen sie sysdba User_Name;

Erstellen der Repository-Datenbankinstanz

Die Repository-Datenbankinstanz ist eine Oracle-Datenbank, in der Sie das SnapManager-Repository erstellen. Die Repository-Datenbankinstanz muss eine eigenständige Datenbank sein und kann nicht die Zieldatenbank sein.

Sie benötigen eine Oracle-Datenbank und ein Benutzerkonto, um auf die Datenbank zugreifen zu können.

1. Melden Sie sich bei SQL an *Plus: Sqlplus '/ AS sysdba'
2. Erstellen Sie einen neuen Tablespace für das SnapManager-Repository: Erstellen Sie Tablespacetablespace_Name-Datendatei '/u01/App/oracle/oradata/Datafile/tablespace_Name.dbf' size 100M autoExtend auf;

   Tablespace_Name ist der Name des Tablespaces.

3. Überprüfen Sie die Blockgröße des Tablespaces: Wählen Sie Tablespace_Name, Block_size aus dba_Tablespaces;

   SnapManager erfordert für den Tablespaces eine Blockgröße von mindestens 4 KB.

Verwandte Informationen

"Technischer Bericht 3761: SnapManager für Oracle: Best Practices"

Erstellen eines Oracle-Benutzers für die Repository-Datenbankinstanz

Ein Oracle-Benutzer ist erforderlich, um sich bei der Repository-Datenbankinstanz anzumelden und auf diese zuzugreifen. Sie müssen diesen Benutzer mit den Berechtigungen *connect* und_Resource_ erstellen.

1. Melden Sie sich bei SQL an *Plus: Sqlplus '/ AS sysdba'
2. Erstellen Sie einen neuen Benutzer, und weisen Sie diesem Benutzer ein Administratorpasswort zu: Erstellen Sie useruser_Name, identifiziert durch admin_password Standard Tablespace_Name Quota unlimited on to tablespace_Name;
   - User_Name ist der Name des Benutzers, den Sie für die Repository-Datenbank erstellen.
   - Admin_password ist das Passwort, das Sie dem Benutzer zuweisen möchten.
   - Tablespace_Name ist der Name des Tablespaces, der für die Repository-Datenbank erstellt wurde.
3. Dem neuen Oracle-Benutzer *connect* und *Resource* Berechtigungen zuweisen: Verbindung gewähren, Ressource zu User_Name zuweisen;

Überprüfen der Oracle Listener-Konfiguration

Der Listener ist ein Prozess, der Client-Verbindungsanforderungen abhört. Es empfängt eingehende Client-Verbindungsanfragen und verwaltet den Datenverkehr dieser Anfragen an die Datenbank. Bevor Sie eine Verbindung zu einer Zieldatenbank oder einer Repository-Datenbankinstanz herstellen, können Sie mit dem STATUS-Befehl die Listener-Konfiguration überprüfen.

Der STATUS-Befehl zeigt grundlegende Statusinformationen zu einem bestimmten Listener an, einschließlich einer Zusammenfassung der Listener-Konfigurationseinstellungen, Listener-Protokolladressen und einer Zusammenfassung der bei diesem Listener registrierten Dienste.

1. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `lsnrctl STATUS`

   Der dem Listener-Port zugewiesene Standardwert ist 1521.

SnapManager wird installiert

Sie müssen SnapManager auf jedem Host installieren, auf dem die Datenbank, die Sie sichern möchten, ausgeführt wird.

Sie müssen SnapDrive für UNIX auf dem Datenbank-Host installiert und eine Verbindung zum Speichersystem hergestellt haben.

Informationen zum Installieren SnapDrive und Herstellen einer Verbindung zum Storage-System finden Sie in der Dokumentation von SnapDrive für UNIX.

Sie müssen eine SnapManager-Instanz pro Datenbank-Host installieren. Wenn Sie eine RAC-Datenbank (Real Application Cluster) verwenden und die RAC-Datenbank sichern möchten, müssen Sie SnapManager auf allen Hosts der RAC-Datenbank installieren.

1. Laden Sie das SnapManager für Oracle Installationspaket für UNIX von der NetApp Support Site herunter und kopieren Sie es auf das Host-System.

   "NetApp Downloads: Software"

2. Melden Sie sich beim Datenbank-Host als Root-Benutzer an.
3. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie das Installationspaket kopiert haben.

4. Machen Sie das Installationspaket ausführbar: Chmod 755install_package.bin
5. Installieren Sie SnapManager: ./install_package.bin
6. Drücken Sie die Eingabetaste, um fortzufahren.
7. Führen Sie folgende Schritte aus:

   a. Drücken Sie die Eingabetaste, um den Standardwert für den Benutzer des Betriebssystems zu übernehmen.

      der Standardwert für den Benutzer ist oracle.

   b. Drücken Sie die Eingabetaste, um den Standardwert für die Betriebssystemgruppe zu übernehmen.

      Der Standardwert für die Gruppe ist dba.

   c. Drücken Sie die Eingabetaste, um den Standardwert für den Starttyp zu übernehmen.

   Die Konfigurationsübersicht wird angezeigt.

8. Überprüfen Sie die Konfigurationsübersicht, und drücken Sie die Eingabetaste, um fortzufahren.

   SnapManager ist unter /opt/NTAPsmo für Solaris und /opt/NetApp/ für alle anderen UNIX-Hosts installiert.

Verwandte Informationen

Einrichtung von SnapManager

"NetApp Dokumentation: SnapDrive für UNIX"

Einrichtung von SnapManager

Sie können SnapManager starten und entweder über die Benutzeroberfläche (UI) oder die Befehlszeilenschnittstelle (CLI) darauf zugreifen. Nach dem Zugriff auf SnapManager müssen Sie das SnapManager-Repository erstellen, bevor Sie SnapManager-Vorgänge durchführen.

Starten des SnapManager-Servers

Sie müssen den SnapManager-Server vom Ziel-Datenbank-Host starten.

1. Melden Sie sich beim Ziel-Datenbank-Host an und starten Sie den SnapManager-Server: `smo_server start`

   Die folgende Meldung wird angezeigt: SnapManager-Server wurde auf sicherem Port_number mit PID PID_number gestartet.

   Der Standardport ist 27214.

Sie können überprüfen, ob SnapManager ordnungsgemäß ausgeführt wird: smo System Verify

Die folgende Meldung wird angezeigt: Operation ID Operation_ID_number erfolgreich.

Zugriff auf die SnapManager Benutzeroberfläche

Sie können die SnapManager-Benutzeroberfläche (UI) Remote über einen Webbrowser von jedem System aus aufrufen, das auf einem von SnapManager unterstützten Betriebssystem ausgeführt wird. Sie können auch über den Ziel-Datenbank-Host auf die SnapManager-Benutzeroberfläche zugreifen, indem Sie den smogui-Befehl ausführen.

- Sie müssen sicherstellen, dass SnapManager ausgeführt wird.
- Sie müssen sicherstellen, dass das unterstützte Betriebssystem und Java auf dem System installiert sind, auf dem Sie auf die SnapManager-Benutzeroberfläche zugreifen möchten.

  Informationen zum unterstützten Betriebssystem und Java finden Sie im Interoperabilitäts-Matrix-Tool.

  a. Geben Sie im Webbrowser-Fenster folgende Eingabe ein: https://server_name.domain.com:port_number
     - Server_Name ist der Name des Ziel-Datenbank-Hosts, auf dem SnapManager installiert ist.

       Sie können auch die IP-Adresse des Ziel-Datenbank-Hosts eingeben.

     - Port_number ist der Port, auf dem SnapManager ausgeführt wird.

       Der Standardwert ist 27214.

  b. Klicken Sie auf den Link **SnapManager für Oracle starten**.

     Die Benutzeroberfläche von SnapManager für Oracle wird angezeigt.

SnapManager-Repository wird konfiguriert

Sie müssen das SnapManager-Repository in der Repository-Datenbankinstanz konfigurieren. Die Repository-Datenbank speichert Metadaten für Datenbanken, die von SnapManager gemanagt werden.

- Sie müssen die Repository-Datenbankinstanz erstellt haben.
- Sie müssen den Oracle-Benutzer für die Repository-Datenbankinstanz mit den erforderlichen Berechtigungen erstellt haben.
- Sie müssen die Details der Repository-Datenbankinstanz in die Datei nsnames.ora enthalten haben.

Sie können das SnapManager-Repository entweder über die SnapManager-Benutzeroberfläche (UI) oder über die Befehlszeilenschnittstelle (CLI) konfigurieren. Mit diesen Schritten wird das Erstellen eines Repositorys mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es bevorzugen.

Informationen zum Erstellen des Repositorys mithilfe von CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie im linken Bereich der SnapManager-Benutzeroberfläche mit der rechten Maustaste auf **Repositories**.
2. Wählen Sie **Neues Repository erstellen** und klicken Sie auf **Weiter**.
3. Geben Sie im Fenster Repository-Datenbankkonfigurationsinformationen die folgenden Informationen ein:

In diesem Feld…	Tun Sie das…
Benutzername	Geben Sie den Namen des Benutzers ein, den Sie für die Repository-Datenbankinstanz erstellt haben.
Passwort	Geben Sie das Passwort ein.
Gastgeber	Geben Sie die IP-Adresse des Hosts ein, auf dem die Repository-Datenbankinstanz erstellt wird.
Port	Geben Sie den Port ein, der für die Verbindung zur Repository-Datenbankinstanz verwendet wird. Der Standardport ist 1521.
Dienstname	Geben Sie den Namen ein, den SnapManager für die Verbindung zur Repository-Datenbankinstanz verwendet. Je nach den Details in der Datei nsnames.ora kann es sich um den kurzen Servicenamen oder den vollqualifizierten Servicenamen handelt. +

4. Überprüfen Sie im Fenster Projektarchiv hinzufügen die Konfigurationszusammenfassung und klicken Sie auf **Hinzufügen**.

   Wenn der Vorgang fehlschlägt, klicken Sie auf die Registerkarte **Operationsinformationen**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat. Die Fehlerdetails werden auch im Betriebsprotokoll unter /var/log/smo erfasst.

5. Klicken Sie Auf **Fertig Stellen**.

   Das Repository wird im linken Fensterbereich unter dem Baum **Repositories** aufgelistet. Wenn das Repository nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf **Repositories** und klicken Sie auf **Aktualisieren**.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Vorbereiten der Speichersysteme für die SnapMirror- und SnapVault-Replizierung

SnapManager mit Data ONTAP SnapMirror Technologie kann verwendet werden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Dank der Data ONTAP SnapVault Technologie können Backups effizient auf der Festplatte archiviert werden. Bevor Sie diese Aufgaben in SnapManager ausführen können, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

Eine SnapMirror Beziehung und eine SnapVault Beziehung können auf demselben Clustered Data ONTAP Quell-Volume nicht konfiguriert werden. Sie müssen diese Beziehungen auf verschiedenen Quell-Volumes konfigurieren.

Verwandte Informationen

Verständnis der Unterschiede zwischen SnapMirror und SnapVault

Vorbereiten der Storage-Systeme für die SnapMirror Replizierung

Storage-Systeme werden für die SnapVault-Replizierung vorbereitet

Verständnis der Unterschiede zwischen SnapMirror und SnapVault

SnapMirror ist eine Disaster-Recovery-Technologie für den Failover von primärem Storage zu sekundärem Storage an einem geografisch verteilten Standort. SnapVault ist eine Archivierungstechnologie für die Disk-to-Disk Snapshot Kopie-Replizierung, die für Compliance-Standards und andere Governance-Zwecke entwickelt wurde.

Diese Ziele berücksichtigen das unterschiedliche Gleichgewicht, das jede Technologie zwischen den Zielen der Backup-Währung und der Backup-Aufbewahrung findet:

- SnapMirror speichert _nur die Snapshot Kopien, die sich im Primär-Storage befinden, da bei einem Ausfall ein Failover zur neuesten Version der Primärdaten erforderlich sein muss, von der Sie wissen, dass sie gut sind. Beispielsweise könnte Ihr Unternehmen stündliche Kopien von Produktionsdaten über einen Zeitraum von zehn Tagen spiegeln. Wie der Anwendungsfall des Failovers schon andeutet, muss die Ausrüstung auf dem Sekundärsystem äquivalent oder nahezu identisch mit der Ausrüstung auf dem Primärsystem sein, um Daten effizient aus dem gespiegelten Storage bereitzustellen.
- Im Gegensatz dazu speichert SnapVault Snapshot Kopien *unabhängig davon, ob sie sich derzeit im Primärspeicher befinden oder nicht*, weil im Rahmen eines Audits wahrscheinlich der Zugriff auf historische Daten so wichtig ist wie der Zugriff auf aktuelle Daten. Vielleicht möchten Sie monatlich Snapshot Kopien Ihrer Daten über einen Zeitraum von 20 Jahren aufbewahren (z. B. um gesetzliche Buchhaltungsvorschriften für Ihr Unternehmen einzuhalten). Da keine Daten aus dem sekundären Speicher bereitgestellt werden müssen, können Sie langsamere, kostengünstigere Festplatten auf dem Vault-System verwenden.

Natürlich geben die verschiedenen Gewichte, die SnapMirror und SnapVault der Backup-Währung und der Backup-Aufbewahrung geben, letztlich vom Limit der 255-Snapshot-Kopien für jedes Volume ab. Bei Beibehaltung der neuesten Kopien bei SnapMirror werden die Kopien, die im Laufe der längsten Zeit erstellt wurden, von SnapVault aufbewahrt.

Vorbereiten der Storage-Systeme für die SnapMirror Replizierung

Bevor Sie die integrierte SnapMirror Technologie von SnapManager zur Spiegelung von Snapshot Kopien verwenden können, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und dann die Beziehung initialisieren. Bei der Initialisierung erstellt SnapMirror eine Snapshot Kopie des Quell-Volume, dann überträgt die Kopie und alle Datenblöcke, auf die sie Bezug nimmt auf das Ziel-Volume. Es überträgt außerdem alle anderen, weniger neuesten Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume.

- Sie müssen die Quell- und Ziel-Volumes in Peering Clustern mit Peering Storage Virtual Machines (SVMs) erstellen. Weitere Informationen finden Sie im *Clustered Data ONTAP Cluster Peering Express Guide*.
- Sie müssen ein Cluster-Administrator sein.
- Für die Überprüfung von Snapshot Kopien auf dem Ziel-Volume müssen die Storage Virtual Machines (SVMs) aus Quell- und Ziel-Storage über eine Management-LIF und eine Daten-LIF verfügen. Die Management-LIF muss den gleichen DNS-Namen wie die SVM aufweisen. Legen Sie die Management-LIF-Rolle auf Daten, das Protokoll none und die Firewall-Richtlinie auf das Management fest.

Sie können eine SnapMirror Beziehung mit der Data ONTAP Befehlszeilenschnittstelle (CLI) oder OnCommand System Manager erstellen. Bei der folgenden Vorgehensweise wird vorausgesetzt, dass Sie die CLI verwenden. Informationen zum Erstellen der SnapMirror Beziehung mithilfe von OnCommand System Manager finden Sie im *Clustered Data ONTAP Volume Disaster Recovery Preparation Express Guide*.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapMirror Beziehung:

1. Ermitteln des Ziel-Clusters
2. Verwenden Sie für das Ziel-Cluster den Befehl Volume create mit der Option -typeDP, um ein SnapMirror Ziel-Volume zu erstellen, das entweder die gleiche oder eine größere Größe als das Quell-Volume hat.

   Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

   Mit dem folgenden Befehl wird ein 2-GB-Ziellaufwerk namens dstvolB in SVM2 auf dem Aggregat node01_aggr erstellt:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -type DP
   -size 2GB
   ```

3. Verwenden Sie für die Ziel-SVM den befehl „snapmirror create“ mit dem Parameter „-type DP“, um eine SnapMirror-Beziehung zu erstellen.

   Der DP-Typ definiert die Beziehung als SnapMirror-Beziehung.

   Der folgende Befehl erstellt eine SnapMirror Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2. Standardmäßig weist der Befehl die SnapMirror Standard-Richtlinie DPStandard zu:

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path
   SVM2:dstvolB
   -type DP
   ```

   Definieren Sie keinen Spiegelungsplan für die SnapMirror Beziehung. SnapManager tut dies für Sie beim Erstellen eines Backup-Zeitplans.

   Wenn Sie die SnapMirror Standardrichtlinie nicht verwenden möchten, können Sie den Befehl zum Erstellen der snapmirror-Richtlinie aufrufen, um eine SnapMirror-Richtlinie zu definieren.

4. Verwenden Sie den snapmirror Initialize-Befehl, um die Beziehung zu initialisieren.

   Bei der Initialisierung wird ein Basistransfer zum Ziel-Volume durchgeführt. SnapMirror erstellt eine Snapshot-Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die er auf das Ziel-Volume verweist. Sie überträgt zudem alle anderen Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume.

   Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2 initialisiert:

   ```
   SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

Verwandte Informationen

"Clustered Data ONTAP 8.3 Cluster Peering Express Guide"

"Clustered Data ONTAP 8.3 Volume Disaster Recovery Preparation Express Guide"

Storage-Systeme werden für die SnapVault-Replizierung vorbereitet

Bevor Sie die integrierte SnapVault Technologie von SnapManager zur Archivierung von Snapshot Kopien auf Festplatte verwenden können, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und dann die Beziehung initialisieren. Bei der Initialisierung erstellt SnapVault eine Snapshot Kopie des Quell-Volume, überträgt dann die Kopie und alle Datenblöcke, auf die sie auf das Ziel-Volume verweist.

- Sie müssen die Quell- und Ziel-Volumes in Peering Clustern mit Peering Storage Virtual Machines (SVMs) erstellen. Weitere Informationen finden Sie im *Clustered Data ONTAP Cluster Peering Express Guide*.
- Sie müssen ein Cluster-Administrator sein.

Sie können SnapVault Beziehungen mit der Data ONTAP Befehlszeilenschnittstelle (CLI) oder mit OnCommand System Manager erstellen. Bei der folgenden Vorgehensweise wird vorausgesetzt, dass Sie die CLI verwenden. Informationen zur Erstellung der SnapVault Beziehung mithilfe von OnCommand System Manager finden Sie im *Clustered Data ONTAP Volume Backup Using SnapVault Express Guide*.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapVault Beziehung:

1. Ermitteln des Ziel-Clusters
2. Verwenden Sie für das Ziel-Cluster den Befehl Volume create mit der Option -typeDP, um ein SnapVault Ziel-Volume zu erstellen, das mindestens dieselbe Größe hat als das Quell-Volume.

   Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

   Mit dem folgenden Befehl wird ein 2-GB-Ziellaufwerk namens dstvolB in SVM2 auf dem Aggregat node01_aggr erstellt:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -type DP
-size 2GB
```

3. Verwenden Sie auf der Ziel-SVM den Erstellungsbefehl für die snapmirror Richtlinie, um eine SnapVault-Richtlinie zu erstellen.

   Mit dem folgenden Befehl wird die SVM-weite Richtlinie SVM1-Vault erstellt:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-vault
```

   Für die SnapVault-Beziehung dürfen keine Cron-Zeitpläne oder Snapshot-Kopierrichtlinien definiert werden. SnapManager tut dies für Sie beim Erstellen eines Backup-Zeitplans.

4. Mit dem Befehl „SnapMirror Policy add-rule“ können Sie der Richtlinie eine Regel hinzufügen, die die folgenden Beschriftungen für Snapshot Kopien und die Aufbewahrungsrichtlinie für jedes Etikett definiert:
   - Täglich
   - Wöchentlich
   - Monatlich
   - Stündlich
   - Unbegrenzt * wichtig:* die Etiketten sind Groß- und Kleinschreibung.

     Dies sind feste Etiketten, die SnapManager verwendet. Bei der Archivierung eines Backups wählen Sie eine dieser Optionen aus. Sie müssen diesen Befehl einmal für jede der Regeln ausführen, die Sie hinzufügen.

     + der folgende Befehl fügt eine Regel zur SVM1-Vault-Richtlinie hinzu, die das Label „`daily`“ definiert und gibt an, dass dreißig Snapshot-Kopien, die mit dem Label übereinstimmen, im Tresor aufbewahrt werden sollten:

```
SVM2::> snapmirror policy add-rule -vserver SVM2 -policy SVM1-vault
-snapmirror-label Daily -keep 30
```

1. Verwenden Sie den snapmirror create-Befehl mit dem Parameter -type XDP und dem Parameter -Policy, um eine SnapVault-Beziehung zu erstellen und eine Vault-Richtlinie zuzuweisen.

   Der XDP-Typ definiert die Beziehung als eine SnapVault-Beziehung.

   Mit dem folgenden Befehl wird eine SnapVault-Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2 erstellt. Sie weist die Richtlinie SVM1-Vault zu:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path
SVM2:dstvolB
-type XDP -policy SVM1-vault
```

2. Verwenden Sie den snapmirror Initialize-Befehl, um die Beziehung zu initialisieren.

   Bei der Initialisierung wird ein Basistransfer zum Ziel-Volume durchgeführt. SnapMirror erstellt eine Snapshot-Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die er auf das Ziel-Volume verweist.

   Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume srcvolA auf SVM1 und dem Ziel-Volume dstvolB auf SVM2 initialisiert:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Verwandte Informationen

"Clustered Data ONTAP 8.3 Cluster Peering Express Guide"

"Clustered Data ONTAP 8.3 Volume Backup Using SnapVault Express Guide"

Sichern und Überprüfen Ihrer Datenbanken

Nach der Installation von SnapManager können Sie ein Basis-Backup Ihrer Datenbank erstellen und überprüfen, ob das Backup keine beschädigten Dateien enthält.

Verwandte Informationen

SnapManager Backup – Überblick

Backup-Strategie definieren

Erstellen eines Profils für Ihre Datenbank

Sichern Ihrer Datenbank

Datenbank-Backups werden überprüft

Planung wiederkehrender Backups

SnapManager Backup – Überblick

SnapManager erstellt mithilfe von NetApp Snapshot Technologie die Backups von Datenbanken. Sie können das DBVERIFY-Dienstprogramm verwenden oder SnapManager verwenden, um die Integrität der Backups zu überprüfen.

SnapManager sichert eine Datenbank, indem Snapshot Kopien der Volumes erstellt werden, die Datendateien, Kontrolldateien und Archivprotokolldateien enthalten. Diese Snapshot Kopien bestehen zusammen aus einem Backup-Set, mit dem SnapManager eine Datenbank wiederherstellen kann.

Backup-Strategie definieren

Wenn Sie eine Backup-Strategie vor der Erstellung Ihrer Backups definieren, stellen Sie sicher, dass Ihnen Backups zur erfolgreichen Wiederherstellung Ihrer Datenbanken zur Verfügung stehen. SnapManager bietet einen flexiblen, granularen Backup-Zeitplan, der Ihr Service Level Agreement (SLA) erfüllt.

Informationen zu den Best Practices für SnapManager finden Sie unter *TR 3761*.

Welcher Modus für SnapManager Backups benötigen Sie?

SnapManager unterstützt zwei Backup-Modi:

Backup-Modus	Beschreibung
Online-Backup	Erstellt ein Backup der Datenbank, wenn sich die Datenbank im Online-Status befindet. Dieser Backup-Modus wird auch als Hot Backup bezeichnet.
Offline-Backup	Erstellt eine Sicherung der Datenbank, wenn sich die Datenbank entweder im angehängten oder abschaltenden Zustand befindet. Dieser Backup-Modus wird auch als Cold Backup bezeichnet.

Welche Art von SnapManager-Backup benötigen Sie?

SnapManager unterstützt drei Arten von Backups:

Backup-Typ	Beschreibung
Vollständiges Backup	Erstellt ein Backup der gesamten Datenbank, die alle Datendateien, Kontrolldateien und Archivprotokolldateien umfasst.
Teilweise Sicherung	Erstellt ein Backup ausgewählter Datendateien, Kontrolldateien, Tablespaces und Archivprotokolldateien
Backup nur für Archivierung	Erstellt eine Sicherung nur der Archivprotokolldateien.Sie müssen beim Erstellen des Profils **Archivprotokolle separat** auswählen.

Was für ein Datenbankprofil benötigen Sie?

SnapManager erstellt Backups basierend darauf, ob das Datenbankprofil die Archiv-Log-Backups von den Datendatei-Backups trennt.

Profiltyp	Beschreibung

Ein einzelnes Datenbankprofil für eine kombinierte Sicherung von Datendateien und Archivprotokollen	Ermöglicht Ihnen das Erstellen von: • Vollständige Sicherung mit allen Datendateien, Archivprotokolldateien und Kontrolldateien • Partielles Backup mit ausgewählten Datendateien, Tablespaces, Archivprotokolldateien und Kontrolldateien
Separate Datenbankprofile für Backups von Archivierungsprotokolldaten und Datendatei-Backups	Ermöglicht Ihnen das Erstellen von: • Kombiniertes Backup mit unterschiedlichen Kennungen für Backup von Datendateien und Backup von Archivierungsprotokolldaten • Datendatei-only-Backup aller Datendateien zusammen mit den Kontrolldateien • Partielles, datenonly Backup von ausgewählten Datendateien oder Tablespaces zusammen mit den Control Files • Backup nur bei Archivierung und Protokollen

Welche Namenskonventionen sollten für Snapshot Kopien verwendet werden?

Von Backups erstellte Snapshot Kopien können einer benutzerdefinierten Namenskonvention folgen. Benutzerdefinierte Text oder integrierte Variablen wie der Profilname, der Datenbankname und die von SnapManager bereitgestellte Datenbank-SID können zur Erstellung der Namenskonvention verwendet werden. Sie können die Namenskonvention erstellen, während Sie die Richtlinie erstellen.

Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

Die Namenskonventionen für Snapshot Kopien können während oder nach der Erstellung eines Profils geändert werden. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Vorhandene Snapshot Kopien behalten das vorherige Muster bei.

Wie lange möchten Sie Backup-Kopien auf dem primären Storage-System und dem sekundären Storage-System aufbewahren?

In einer Backup-Aufbewahrungsrichtlinie wird die Anzahl der erfolgreichen Sicherungskopien festgelegt, die aufbewahrt werden sollen. Sie können die Aufbewahrungsrichtlinie angeben, während Sie die Richtlinie erstellen.

Sie können stündlich, täglich, wöchentlich, monatlich oder unbegrenzt als Aufbewahrungsklasse auswählen. Sie können für jede Aufbewahrungsklasse den Aufbewahrungszähler und die Aufbewahrungsdauer entweder gemeinsam oder einzeln festlegen.

- Die Anzahl der Aufbewahrung bestimmt die Mindestanzahl der Backups einer bestimmten Aufbewahrungsklasse, die beibehalten werden soll.

  Wenn beispielsweise der Backup-Zeitplan *Daily* lautet und die Anzahl der Aufbewahrung *10* ist, werden 10 tägliche Backups aufbewahrt.

Die maximale Anzahl von Snapshot Kopien, die Sie mit Data ONTAP aufbewahren können, ist 255. Nach Erreichen des maximalen Limits schlägt die Erstellung neuer Snapshot Kopien standardmäßig fehl. Sie können jedoch die Rotationsrichtlinie in Data ONTAP konfigurieren, um ältere Snapshot-Kopien zu löschen.

- Die Aufbewahrungsdauer legt die Mindestanzahl an Tagen fest, für die das Backup aufbewahrt werden soll.

  Wenn beispielsweise der Backup-Zeitplan *täglich* lautet und die Aufbewahrungsdauer *10* beträgt, werden täglich 10 Tage Backups aufbewahrt.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

Zur langfristigen Aufbewahrung von Backup-Kopien sollten Sie SnapVault verwenden.

Möchten Sie Backup-Kopien mithilfe des Quell-Volume oder eines Ziel-Volume überprüfen?

Wenn Sie SnapMirror oder SnapVault einsetzen, können Sie Backup-Kopien mithilfe der Snapshot-Kopie auf dem SnapMirror oder SnapVault Ziel-Volume überprüfen anstelle der Snapshot-Kopie auf dem primären Storage-System. Die Verwendung eines Ziel-Volumes zur Verifizierung reduziert die Last auf dem primären Storage-System.

Verwandte Informationen

"Technischer Bericht 3761: SnapManager für Oracle: Best Practices"

Erstellen eines Profils für Ihre Datenbank

Sie müssen ein Profil erstellen, damit Ihre Datenbank alle Vorgänge in dieser Datenbank ausführen kann. Das Profil enthält Informationen über die Datenbank und kann nur auf eine Datenbank verweisen. Eine Datenbank kann jedoch durch mehrere Profile referenziert werden. Ein Backup, das mit einem Profil erstellt wird, kann nicht von einem anderen Profil aus aufgerufen werden, auch wenn beide Profile mit derselben Datenbank verknüpft sind.

Sie müssen sicherstellen, dass die Details der Zieldatenbank in der Datei /etc/oratab enthalten sind.

Mit diesen Schritten wird die Erstellung eines Profils für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es bevorzugen.

Informationen zum Erstellen von Profilen mithilfe der CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie in der Repository-Struktur mit der rechten Maustaste auf das Repository oder den Host und wählen Sie **Profil erstellen** aus.
2. Geben Sie auf der Seite Profilkonfigurationsinformationen den benutzerdefinierten Namen und das Kennwort für das Profil ein.
3. Geben Sie auf der Seite Datenbankkonfigurationsinformationen die folgenden Informationen ein:

In diesem Feld…	Tun Sie das…
Datenbankname	Geben Sie den Namen der Datenbank ein, die Sie sichern möchten.
• Datenbank-SID*	Geben Sie die sichere ID (SID) der Datenbank ein. Der Datenbankname und die Datenbank-SID können identisch sein.
Gastgeber	Geben Sie die IP-Adresse des Hosts ein, auf dem sich die Zieldatenbank befindet. Sie können auch den Hostnamen angeben, wenn der Hostname im Domain Name System (DNS) angegeben ist.
Host-Konto	Geben Sie den Oracle-Benutzernamen der Zieldatenbank ein. der Standardwert für den Benutzer ist oracle.
Host-Gruppe	Geben Sie den Namen der Oracle-Benutzergruppe ein. Der Standardwert ist dba. +

4. Wählen Sie auf der Seite Datenbankverbindungsinformationen eine der folgenden Optionen aus:

Wählen Sie diese Option…	Ihr Ziel ist
O/S-Authentifizierung verwenden	Verwenden Sie die vom Betriebssystem gepflegten Anmeldeinformationen, um Benutzer zu authentifizieren, die auf die Datenbank zugreifen.
Datenbankauthentifizierung Verwenden	Erlauben Sie Oracle, einen administrativen Benutzer mithilfe der Authentifizierung von Kennwortdateien zu authentifizieren. Geben Sie die entsprechenden Informationen zur Datenbankverbindung ein. • Geben Sie im Feld **SYSDBA Privileged User Name** den Namen des Datenbankadministrators mit Administratorrechten ein. • Geben Sie im Feld **Passwort** das Passwort des Datenbankadministrators ein. • Geben Sie im Feld **Port** die Portnummer ein, die für die Verbindung mit dem Host verwendet wird, auf dem sich die Datenbank befindet. Der Standardwert ist 1521.

Verwendung der ASM-Instanz-Authentifizierung	Zulassen, dass die ASM-Datenbankinstanz einen administrativen Benutzer authentifiziert. Geben Sie die entsprechenden Authentifizierungsdaten für die ASM-Instanz ein. • Geben Sie im Feld **SYSDBA/SYSASM Privileged User Name** den Benutzernamen des ASM-Instanzadministrators mit Administratorrechten ein. • Geben Sie im Feld **Passwort** das Passwort des Administrators ein.

Hinweis: Sie können den ASM-Authentifizierungsmodus nur auswählen, wenn Sie eine ASM-Instanz auf dem Datenbank-Host haben.

5. Wählen Sie auf der Seite RMAN-Konfigurationsinformationen eine der folgenden Optionen aus:

Wählen Sie diese Option…	Wenn…
Verwenden Sie nicht RMAN	Sie verwenden RMAN nicht für das Management von Backup- und Restore-Vorgängen.
Verwenden Sie RMAN über die Steuerdatei	Sie verwalten das RMAN-Repository mit Steuerdateien.
Verwenden Sie RMAN über den Wiederherstellungskatalog	Sie verwalten das RMAN-Repository mithilfe der Recovery-Katalogdatenbank. Geben Sie den Benutzernamen ein, der Zugriff auf die Datenbank des Wiederherstellungspatalogs, das Kennwort und den Oracle-Nettodienstnamen der Datenbank hat, die die TNS-Verbindung (Transparent Network Substrat) verwaltet. +

6. Wählen Sie auf der Seite Snapshot Naming Information die Variablen aus, um ein Benennungsformat für die Snapshot Kopie anzugeben.

   Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

7. Führen Sie auf der Seite Richtlinieneinstellungen folgende Schritte durch:
   a. Geben Sie Anzahl und Dauer der Aufbewahrung für jede Aufbewahrungsklasse ein.
   b. Wählen Sie aus der Dropdown-Liste **Schutzrichtlinie** die Schutzrichtlinie aus.

      Je nachdem, ob SnapMirror oder SnapVault Beziehung aufgebaut ist, müssen Sie entweder *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* Richtlinien auswählen.

   c. Wenn Sie Archivprotokolle separat sichern möchten, aktivieren Sie das Kontrollkästchen **Archivprotokolle separat sichern**, legen Sie die Aufbewahrung fest und wählen Sie die Schutzrichtlinie aus.

Sie können eine Richtlinie auswählen, die sich von der für Datendateien verknüpften Richtlinie unterscheidet. Wenn Sie beispielsweise *SnapManager_cDOT_Mirror* für Datendateien ausgewählt haben, können Sie *SnapManager_cDOT_Vault* für Archivprotokolle auswählen.

8. Geben Sie auf der Seite Benachrichtigungseinstellungen konfigurieren die Einstellungen für E-Mail-Benachrichtigungen an.
9. Wählen Sie auf der Seite Verlaufsdaten-Konfigurationsinformationen eine der Optionen aus, um den Verlauf der SnapManager-Vorgänge beizubehalten.
10. Überprüfen Sie auf der Seite Vorgang „Profil erstellen“ die Informationen und klicken Sie auf **Erstellen**.
11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

    Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Sichern Ihrer Datenbank

Nachdem Sie ein Profil erstellt haben, müssen Sie Ihre Datenbank sichern. Sie können wiederkehrende Backups nach der erstmaligen Sicherung und Überprüfung planen.

In diesen Schritten wird gezeigt, wie Sie mithilfe der SnapManager-Benutzeroberfläche ein Backup Ihrer Datenbank erstellen. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden.

Informationen zur Erstellung von Backups mit CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die zu sichernde Datenbank enthält, und wählen Sie **Backup** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

   Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

   Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die override.default.backup.pattern und new.default.backup.pattern Konfigurationsvariablen bearbeiten, um Ihr eigenes Standard-Backup-Label-Muster zu erstellen.

3. In **SnapVault-Label** müssen Sie beim Einrichten der SnapVault-Beziehung das SnapMirror-Label eingeben, das Sie in den Regeln der SnapMirror-Richtlinie angegeben haben.

   Das Feld **SnapVault Label** wird nur angezeigt, wenn Sie beim Erstellen des Profils *SnapManager_cDOT_Vault* als Schutzrichtlinie ausgewählt haben.

4. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

   Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

5. Führen Sie auf der Seite Datenbank, Tablespaces oder Datendateien zur Datensicherung die folgenden Schritte aus:
   a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
   b. Wählen Sie **Backup Archivelogs** aus, um die Archiv-Log-Dateien separat zu sichern.
   c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.

      Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

   d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

      Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

   e. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

      Wenn Sie Auto auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

   f. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
   g. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.
6. Geben Sie auf der Seite Task Enabling an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.
7. Überprüfen Sie auf der Seite Backup-Vorgang durchführen die Informationen und klicken Sie auf **Backup**.
8. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

   Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Datenbank-Backups werden überprüft

Sie können die Sicherung Ihrer Datenbank überprüfen, um sicherzustellen, dass die gesicherten Dateien nicht beschädigt sind.

Wenn Sie beim Erstellen eines Backups nicht das Kontrollkästchen **Backup überprüfen mit dem Dienstprogramm Oracle DBVERIFY** aktiviert haben, müssen Sie diese Schritte manuell durchführen, um die Sicherung zu überprüfen. Wenn Sie das Kontrollkästchen aktiviert haben, überprüft SnapManager das Backup automatisch.

1. Wählen Sie aus der Struktur **Repositories** das Profil aus.
2. Klicken Sie mit der rechten Maustaste auf das Backup, das Sie überprüfen möchten, und wählen Sie **Überprüfen**.

3. Klicken Sie Auf **Fertig Stellen**.

   Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

   Klicken Sie im Baum **Repository** mit der rechten Maustaste auf das Backup und klicken Sie dann auf **Eigenschaften**, um die Ergebnisse des Verifizierungsvorgangs anzuzeigen.

Sie können gesicherte Dateien verwenden, um Wiederherstellungsvorgänge durchzuführen. Informationen zur Durchführung von Wiederherstellungsvorgängen über die SnapManager-Benutzeroberfläche (UI) finden Sie in der *Online-Hilfe*. Wenn Sie die Befehlszeilenschnittstelle (CLI) zum Durchführen von Wiederherstellungsvorgängen verwenden möchten, finden Sie im *SnapManager für Oracle – Administratorhandbuch für UNIX*.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Planung wiederkehrender Backups

Sie können Backup-Vorgänge so planen, dass die Backups automatisch in regelmäßigen Abständen initiiert werden. SnapManager ermöglicht die Planung von Backups auf Stundenbasis, täglich, wöchentlich, monatlich oder einmalig.

Sie können mehrere Backup-Zeitpläne für eine einzige Datenbank zuweisen. Wenn Sie jedoch mehrere Backups für dieselbe Datenbank planen, müssen Sie sicherstellen, dass die Backups nicht gleichzeitig geplant sind.

Mit diesen Schritten wird das Erstellen eines Backup-Zeitplans für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche (UI) erläutert. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden. Informationen zum Planen von Backups mithilfe der CLI finden Sie im Administratorhandbuch „*SnapManager für Oracle Administration Guide for UNIX*“.

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die Datenbank enthält, für die Sie einen Backup-Zeitplan erstellen möchten, und wählen Sie **Backup planen** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

   Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

   Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die Variablen override.default.backup.pattern und new.default.backup.patternconfiguration bearbeiten, um Ihr eigenes Standard-Backup-Label-Muster zu erstellen.

3. In **SnapVault-Label** müssen Sie beim Einrichten der SnapVault-Beziehung das SnapMirror-Label eingeben, das Sie in den Regeln der SnapMirror-Richtlinie angegeben haben.

   Das Feld **SnapVault Label** wird nur angezeigt, wenn Sie beim Erstellen des Profils *SnapManager_cDOT_Vault* als Schutzrichtlinie ausgewählt haben.

4. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

5. Führen Sie auf der Seite Datenbank, Tablespaces oder Datendateien zur Datensicherung die folgenden Schritte aus:
   a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
   b. Wählen Sie **Backup Archivelogs** aus, um die Archiv-Log-Dateien separat zu sichern.
   c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.

      Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

   d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

      Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

   e. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

      Wenn Sie Auto auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

   f. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
   g. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.
6. Geben Sie im Feld **Terminplanname** einen benutzerdefinierten Namen des Zeitplans ein.

   Sie dürfen keine Leerzeichen in den Namen einfügen.

7. Führen Sie auf der Seite Backup Schedule konfigurieren die folgenden Schritte aus:
   a. Wählen Sie aus der Dropdown-Liste **Durchführung dieser Operation** die Häufigkeit des Backup-Zeitplans aus.
   b. Geben Sie im Feld **Startdatum** das Datum an, an dem Sie den Backup-Zeitplan starten möchten.
   c. Geben Sie im Feld **Startzeit** den Zeitpunkt an, zu dem der Backup-Zeitplan gestartet werden soll.
   d. Geben Sie das Intervall an, in dem Backups erstellt werden sollen.

      Wenn Sie beispielsweise die Frequenz als stündlich ausgewählt haben und das Intervall als 2 angeben, werden die Backups alle 2 Stunden geplant.

8. Geben Sie auf der Seite Task Enabling an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.
9. Überprüfen Sie auf der Seite Backup Schedule Operation durchführen die Informationen und klicken Sie auf **Zeitplan**.
10. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

    Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum

Scheitern verurteilt hat.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Weitere Schritte

Nach der Installation von SnapManager und dem erfolgreichen Erstellen eines Backups können Sie mit SnapManager Wiederherstellungs-, Recovery- und Klonvorgänge durchführen. Zusätzlich erhalten Sie eventuell Informationen zu anderen SnapManager Funktionen, wie zum Beispiel Planung, Management des SnapManager Betriebs und Aufrechterhaltung der Historie von Aktivitäten.

Weitere Informationen zu diesen Funktionen sowie Informationen zur Version von SnapManager finden Sie in der folgenden Dokumentation. Alle Informationen finden Sie im "NetApp Support".

- "SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

  Beschreibt die Konfiguration und Verwaltung von SnapManager für Oracle. Die Themen umfassen das Konfigurieren, Sichern, Wiederherstellen und Klonen von Datenbanken, das Durchführen von Sekundärschutz, Außerdem eine Erläuterung der CLI-Befehle und Anweisungen zum Upgrade und der Deinstallation des Produkts.

- "Versionshinweise zu SnapManager 3.4 für Oracle"

  Beschreibt neue Funktionen, feste Probleme, wichtige Vorsichtsmaßnahmen, bekannte Probleme und Einschränkungen für SnapManager für Oracle.

- *SnapManager für Oracle Online-Hilfe*

  Beschreibt die Schritt-für-Schritt-Verfahren zur Durchführung verschiedener SnapManager-Vorgänge mithilfe der SnapManager-Benutzeroberfläche.

  Die *Online-Hilfe* ist in die SnapManager-Benutzeroberfläche integriert und steht nicht auf der Support-Website zur Verfügung.

- "Technischer Bericht 3761: SnapManager für Oracle: Best Practices"

  Beschreibt die Best Practices von SnapManager für Oracle.

- "NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage"

  Beschreibt Best Practices zur Konfiguration von Oracle Datenbanken auf NetApp Storage-Systemen.

Verwandte Informationen

"NetApp Support"

"NetApp Dokumentation: Produktbibliothek A-Z"

Installations- und Setup-Handbuch für UNIX®

Dieser Leitfaden enthält die ersten Aufgaben, die Sie zur Bereitstellung von SnapManager 3.4.2 für Oracle mit Data ONTAP im 7-Mode in einer UNIX-Umgebung durchführen müssen. Die Themen umfassen die Installation und Konfiguration des Produkts sowie die Sicherung der Datenbanken.

Produktübersicht

Automatisiert und vereinfacht die komplexen, manuellen und zeitaufwändigen Prozesse, die beim Backup, Recovery und Klonen von Oracle Datenbanken anfallen. Mithilfe von SnapManager mit Data ONTAP SnapMirror Technologie können Sie Backup-Kopien auf einem anderen Volume erstellen. Mit der Data ONTAP SnapVault Technologie werden Backups effizient auf Festplatten archiviert.

SnapManager lässt sich mit nativen Oracle Technologien wie Oracle Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) und Direct NFS über FC-, iSCSI- und NFS-Protokolle integrieren. Optional können mit SnapManager erstellte Backups mit dem Oracle Recovery Manager (RMAN) katalogisiert werden, um die Backup-Informationen zu erhalten. Diese Backups können später in Restore-Vorgängen auf Blockebene oder in zeitpunktgenauen Recovery-Vorgängen verwendet werden.

SnapManager Highlights

SnapManager ermöglicht die nahtlose Integration mit Oracle Datenbanken auf dem UNIX Host und über das Backend mit NetApp Snapshot, SnapRestore und FlexClone Technologien Es bietet eine benutzerfreundliche Oberfläche (UI) und eine Befehlszeilenschnittstelle (CLI) für Administrationsfunktionen.

Mit SnapManager können Sie folgende Datenbankvorgänge ausführen und Daten effizient managen:

- Erstellung platzsparender Backups auf primärem oder sekundärem Storage

  SnapManager ermöglicht Ihnen ein separates Backup der Datendateien und die Archivierung von Protokolldateien.

- Planen von Backups
- Wiederherstellung vollständiger oder partieller Datenbanken unter Verwendung eines dateibasierten oder Volume-basierten Restore-Vorgangs
- Wiederherstellung von Datenbanken durch Erkennung, Mounten und Anwendung von Archivprotokolldateien aus Backups
- Beschneiden von Archiv-Log-Dateien von Archiv-Protokollzielen bei der Erstellung von Backups nur der Archivprotokolle
- Automatische Aufbewahrung einer minimalen Anzahl von Archiv-Log-Backups, da nur die Backups gespeichert werden, die eindeutige Archivprotokolldateien enthalten
- Verfolgung von Betriebsdetails und Erstellung von Berichten
- Backup wird überprüft, um sicherzustellen, dass sich Backups in einem gültigen Blockformat befinden und dass keine der gesicherten Dateien beschädigt sind
- Pflegen eines Verlaufs von Vorgängen, die im Datenbankprofil durchgeführt werden

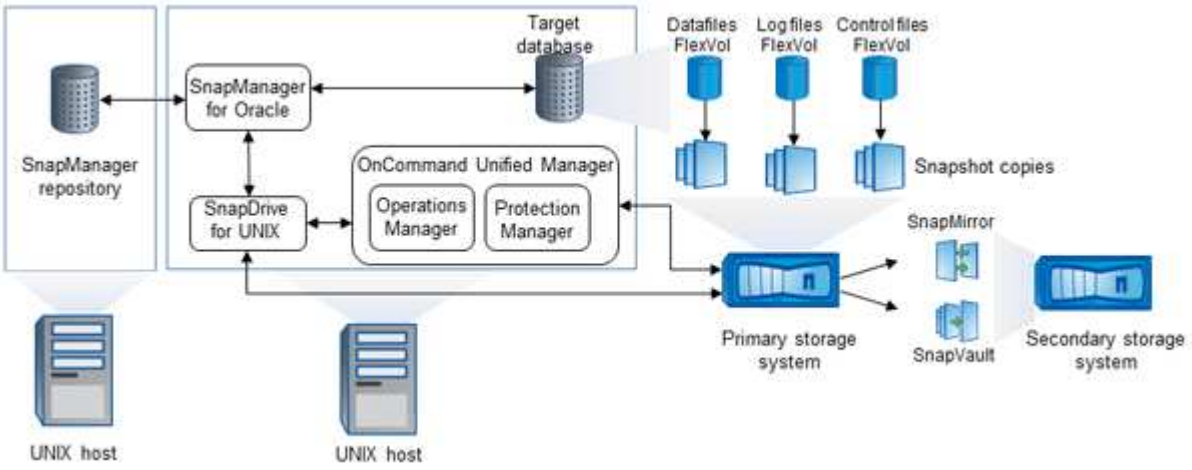
Ein Profil enthält Informationen über die Datenbank, die von SnapManager gemanagt werden soll.

- Sicherung von Backups auf sekundären und tertiären Storage-Systemen.
- Erstellung platzsparender Backup-Klone auf primärem oder sekundärem Storage

SnapManager ermöglicht Ihnen die Aufteilung eines Datenbankklonen.

Architektur von SnapManager

SnapManager für Oracle enthält Komponenten, die gemeinsam eine umfassende und leistungsstarke Backup-, Restore-, Recovery- und Klonlösung für Oracle Datenbanken bieten.



SnapDrive für UNIX

SnapManager benötigt SnapDrive, um die Verbindung zum Storage-System herzustellen. Sie müssen SnapDrive for UNIX auf jedem Ziel-Datenbank-Host installieren, bevor Sie SnapManager installieren.

SnapManager für Oracle

Sie müssen SnapManager für Oracle auf jedem Ziel-Datenbank-Host installieren.

Sie können entweder die Befehlszeilenschnittstelle (CLI) oder die Benutzeroberfläche vom Datenbank-Host verwenden, auf dem SnapManager für Oracle installiert ist. Sie können die SnapManager-Benutzeroberfläche auch Remote verwenden, indem Sie einen Webbrowser von jedem System verwenden, das auf einem von SnapManager unterstützten Betriebssystem ausgeführt wird.

Die unterstützten JRE-Versionen sind 1.5, 1.6, 1.7 und 1.8.

Zieldatenbank

Die Zieldatenbank ist eine Oracle Datenbank, die Sie mit SnapManager managen möchten, indem Sie Backup-, Restore-, Recovery- und Klonvorgänge durchführen.

Die Zieldatenbank kann eine eigenständige Real Application Clusters (RAC) sein oder auf Oracle Automatic Storage Management (ASM)-Volumes residieren. Weitere Informationen zu den unterstützten Oracle Datenbankversionen, Konfigurationen, Betriebssystemen und Protokollen finden Sie im NetApp Interoperabilitäts-Matrix-Tool.

SnapManager Repository

Das SnapManager Repository befindet sich in einer Oracle Datenbank und speichert Metadaten zu Profilen, Backups, Restores, Recoverys und Klonen. Ein einziges Repository kann Informationen über Vorgänge enthalten, die an mehreren Datenbankprofilen durchgeführt werden.

Das SnapManager-Repository kann sich nicht in der Zieldatenbank befinden. Die SnapManager-Repository-Datenbank und die Zieldatenbank müssen online sein, bevor SnapManager Vorgänge durchgeführt werden können.

OnCommand Unified Manager Core-Paket

Das zentrale OnCommand Unified Manager Paket umfasst die Funktionen von Operations Manager, Protection Manager und Provisioning Manager. Sie zentralisiert die Implementierung, das Klonen, Backup und Recovery sowie DR-Richtlinien. Durch die Integration dieser Funktionen können viele Management-Funktionen über ein einzelnes Tool ausgeführt werden.

Operations Manager

Operations Manager ist die webbasierte Benutzeroberfläche (UI) des Kernpakets von OnCommand Unified Manager. Sie wird für das tägliche Storage Monitoring, Problemwarnungen und die Berichterstellung in der Storage- und Storage-System-Infrastruktur genutzt. Die Integration von SnapManager nutzt die RBAC-Funktionen von Operations Manager.

Protection Manager

Protection Manager bietet Administratoren eine benutzerfreundliche Management-Konsole für die schnelle Konfiguration und Steuerung aller SnapMirror- und SnapVault-Vorgänge. Mit dieser Applikation können Administratoren einheitliche Datensicherungsrichtlinien anwenden, komplexe Datensicherungsprozesse automatisieren und Backup- und Replizierungsressourcen bündeln, um eine höhere Auslastung zu erzielen.

Die Schnittstelle für Protection Manager ist die NetApp Management Console, die Client-Plattform für NetApp Management Software-Applikationen. TheNetApp Management Console läuft auf einem Windows- oder Linux-System, das sich von dem Server unterscheidet, auf dem der OnCommand-Server installiert ist. So können Storage-, Applikations- und Serveradministratoren tägliche Aufgaben durchführen, ohne zwischen verschiedenen UIs wechseln zu müssen. Die Applikationen, die in der NetApp Management Console ausgeführt werden, sind Protection Manager, Provisioning Manager und Performance Advisor.

Primärspeicher

SnapManager sichert die Zieldatenbanken auf dem primären NetApp Storage-System.

Sekundäres Storage-System

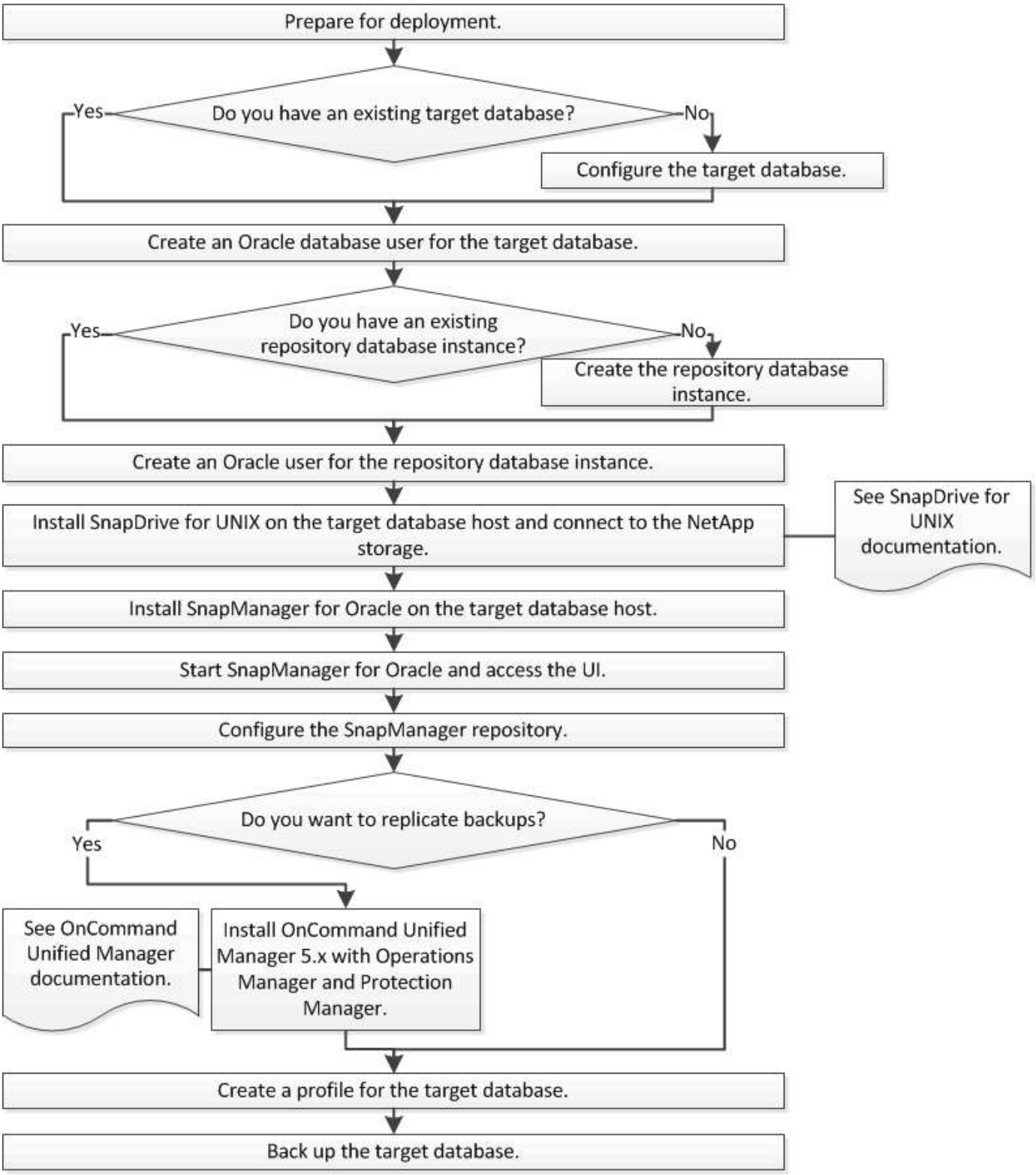
Wenn Sie die Datensicherung in einem Datenbankprofil ermöglichen, werden die Backups, die von SnapManager auf dem primären Storage-System erstellt wurden, mithilfe von SnapVault und SnapMirror Technologien auf ein sekundäres NetApp Storage-System repliziert.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Implementierungs-Workflow

Bevor Sie Backups mit SnapManager erstellen können, müssen Sie zuerst SnapDrive für UNIX installieren und dann SnapManager für Oracle installieren.



Bereitstellung wird vorbereitet

Bevor Sie SnapManager bereitstellen, müssen Sie sicherstellen, dass Ihr Speichersystem und UNIX-Hosts die Mindestanforderungen für die Ressourcen erfüllen.

1. Stellen Sie sicher, dass Sie über die erforderlichen Lizenzen verfügen.
2. Überprüfen Sie die unterstützten Konfigurationen.
3. Überprüfen Sie die unterstützten Speichertypen.
4. Vergewissern Sie sich, dass Ihre UNIX Hosts die SnapManager-Anforderungen erfüllen.

SnapManager Lizenzierung

Zur Aktivierung des SnapManager Betriebs sind eine SnapManager Lizenz und mehrere Storage-System-Lizenzen erforderlich. Die SnapManager Lizenz ist in zwei Lizenzmodellen erhältlich: Lizenzierung pro Server. Bei diesem Modell befindet sich die SnapManager Lizenz auf jedem Datenbank-Host und die Lizenzierung erfolgt pro Storage-System. In diesem Modell befindet sich die SnapManager Lizenz im Storage-System.

Die SnapManager Lizenzanforderungen lauten wie folgt:

Lizenz	Beschreibung	Bei Bedarf
SnapManager pro Server	Eine Host-seitige Lizenz für einen bestimmten Datenbank-Host. Die Lizenzen sind nur für Datenbank-Hosts erforderlich, auf denen SnapManager installiert ist. Für das Storage-System ist keine SnapManager Lizenz erforderlich.	Auf dem SnapManager-Host. Auf primären und sekundären Storage-Systemen ist keine SnapManager-Lizenz erforderlich, wenn die Lizenzierung pro Server verwendet wird.
SnapManager pro Storage-System	Eine Storage-seitige Lizenz, die eine beliebige Anzahl von Datenbank-Hosts unterstützt. Nur erforderlich, wenn Sie keine Serverlizenz auf dem Datenbank-Host verwenden.	Auf primären und sekundären Storage-Systemen.
SnapRestore	Eine erforderliche Lizenz zum Wiederherstellen von Datenbanken durch SnapManager.	Auf primären und sekundären Storage-Systemen. Erforderlich auf SnapVault Zielsystemen, um eine Datei aus einem Backup wiederherzustellen.

Lizenz	Beschreibung	Bei Bedarf
FlexClone	Eine optionale Lizenz zum Klonen von Datenbanken.	Auf primären und sekundären Storage-Systemen.erforderlich auf SnapVault Zielsystemen beim Erstellen von Klonen aus einem Backup.
SnapMirror	Eine optionale Lizenz zum Spiegeln von Backups auf ein Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
SnapVault	Eine optionale Lizenz zur Archivierung von Backups auf einem Ziel-Speichersystem.	Auf primären und sekundären Storage-Systemen.
Protokolle	NFS-, iSCSI- oder FC-Lizenzen sind abhängig vom verwendeten Protokoll erforderlich.	Auf primären und sekundären Storage-Systemen. Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.

Unterstützte Konfigurationen

Die Hosts, auf denen Sie SnapManager installieren, müssen die angegebenen Software-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Vor der Installation oder dem Upgrade von SnapManager müssen Sie die Unterstützung Ihrer Konfiguration überprüfen.

Informationen zu unterstützten Konfigurationen finden Sie im Interoperabilitäts-Matrix-Tool.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Unterstützte Speichertypen

SnapManager unterstützt zahlreiche Storage-Typen sowohl auf physischen als auch auf Virtual Machines. Sie müssen die Unterstützung Ihres Storage-Typs überprüfen, bevor Sie SnapManager installieren oder aktualisieren.

Maschine	Storage-Typ
Physischer Server	• Volumes mit NFS-Anbindung • FC-verbundene LUNs • ISCSI-verbundene LUNs

Maschine	Storage-Typ
VMware ESX	• NFS-Volumes sind direkt mit dem Gastbetriebssystem verbunden • RDM-LUNs auf dem Gastbetriebssystem

UNIX Host-Anforderungen

Sie müssen SnapManager für Oracle auf jedem Host installieren, auf dem eine Oracle Datenbank, die Sie sichern möchten, gehostet wird. Sie müssen sicherstellen, dass Ihre Hosts die Mindestanforderungen für die SnapManager-Konfiguration erfüllen.

- Sie müssen SnapDrive auf dem Datenbank-Host installieren, bevor Sie SnapManager installieren.
- Sie können SnapManager entweder auf physischen oder virtuellen Maschinen installieren.
- Sie müssen dieselbe SnapManager-Version auf allen Hosts installieren, die sich dasselbe Repository teilen.
- Wenn Sie Oracle Databases 11.2.0.2 oder 11.2.0.3 verwenden, müssen Sie Oracle Patch 13366202 installieren.

  Wenn Sie DNFS verwenden, müssen Sie die Patches, die im My Oracle Support (MOS)-Bericht 1495104.1 aufgeführt sind, installieren, um maximale Performance und Stabilität zu erzielen.

Datenbanken werden konfiguriert

Sie müssen mindestens zwei Oracle Datenbanken konfigurieren: Eine Zieldatenbank, die Sie mit SnapManager sichern möchten, und eine Repository-Datenbank zum Speichern der Metadaten der Zieldatenbank. Die Zieldatenbank und die SnapManager Repository-Datenbank müssen konfiguriert und online sein, bevor SnapManager Vorgänge durchgeführt werden können.

Konfigurieren der Zieldatenbank

Die Zieldatenbank ist eine Oracle-Datenbank, die entweder als Standalone, Real Application Clusters (RAC), Automatic Storage Management (ASM) oder als andere unterstützte Kombinationen konfiguriert werden kann.

1. Konfigurieren Sie die Zieldatenbank, indem Sie auf *TR-3633* verweisen.

Verwandte Informationen

"NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage"

Erstellen eines Oracle-Datenbankbenutzers für die Zieldatenbank

Ein Benutzer der Oracle-Datenbank muss sich bei der Datenbank anmelden und SnapManager Vorgänge durchführen. Sie müssen diesen Benutzer mit der Berechtigung *sysdba* erstellen, wenn für die Zieldatenbank kein Benutzer mit der Berechtigung *sysdba*

vorhanden ist.

SnapManager kann jeden Oracle-Benutzer mit der Berechtigung *sysdba* verwenden, die für die Zieldatenbank vorhanden ist. Beispielsweise kann SnapManager den standardmäßigen Benutzer *sys* verwenden. Selbst wenn der Benutzer vorhanden ist, können Sie jedoch einen neuen Benutzer für die Zieldatenbank erstellen und die Berechtigung *sysdba* zuweisen.

Sie können auch die OS-Authentifizierungsmethode verwenden, bei der das Betriebssystem (OS) es der Oracle-Datenbank ermöglicht, die vom Betriebssystem gepflegten Anmeldeinformationen zu verwenden, um Benutzer zur Anmeldung in der Datenbank und zur Durchführung von SnapManager-Vorgängen zu authentifizieren. Wenn Sie über das Betriebssystem authentifiziert sind, können Sie eine Verbindung zur Oracle-Datenbank herstellen, ohne einen Benutzernamen oder ein Kennwort anzugeben.

1. Melden Sie sich bei SQL an *Plus: 'sqlplus / AS sysdba'
2. Erstellen Sie einen neuen Benutzer mit einem Administrator-Passwort: 'Benutzername erstellen, der durch admin_password identifiziert wurde;'

   User_Name ist der Name des Benutzers, den Sie erstellen, und admin_password ist das Passwort, das Sie dem Benutzer zuweisen möchten.
3. Weisen Sie dem neuen Oracle-Benutzer die sysdba-Berechtigung zu: 'Gewähren sie sysdba User_Name;'

Erstellen der Repository-Datenbankinstanz

Die Repository-Datenbankinstanz ist eine Oracle-Datenbank, in der Sie das SnapManager-Repository erstellen. Die Repository-Datenbankinstanz muss eine eigenständige Datenbank sein und kann nicht die Zieldatenbank sein.

Sie benötigen eine Oracle-Datenbank und ein Benutzerkonto, um auf die Datenbank zugreifen zu können.

1. Melden Sie sich bei SQL an *Plus: 'sqlplus / AS sysdba'
2. Erstellen Sie einen neuen Tablespace für das SnapManager-Repository: 'Tablespacetablespace_Name Datafile '/u01/App/oracle/oradata/Datafile/tablespace_Name.dbf' size 100M autoExtend on;'

   Tablespace_Name ist der Name des Tablespaces.
3. Überprüfen Sie die Blockgröße des Tablespaces: 'select Tablespace_Name, Block_size from dba_Tablespaces;'

   SnapManager erfordert für den Tablespaces eine Blockgröße von mindestens 4 KB.

Verwandte Informationen

"Technischer Bericht 3761 von NetApp: 'SnapManager für Oracle: Best Practices'"

Erstellen eines Oracle-Benutzers für die Repository-Datenbankinstanz

Ein Oracle-Benutzer ist erforderlich, um sich bei der Repository-Datenbankinstanz anzumelden und auf diese zuzugreifen. Sie müssen diesen Benutzer mit den Berechtigungen *connect* und_Resource_ erstellen.

1. Melden Sie sich bei SQL an *Plus: 'sqlplus / AS sysdba'

2. Erstellen Sie einen neuen Benutzer, und weisen Sie diesem Benutzer ein Administratorpasswort zu: „Useruser_Name erstellen, identifiziert durch admin_password Standard Tablespace_Name Quota unlimited on to tablespace_Name;“
   - User_Name ist der Name des Benutzers, den Sie für die Repository-Datenbank erstellen.
   - Admin_password ist das Passwort, das Sie dem Benutzer zuweisen möchten.
   - Tablespace_Name ist der Name des Tablespaces, der für die Repository-Datenbank erstellt wurde.
3. Dem neuen Oracle-Benutzer *connect* und *Resource* Berechtigungen zuweisen: 'Verbindung gewähren, Ressource zu User_Name;'

Überprüfen der Oracle Listener-Konfiguration

Der Listener ist ein Prozess, der Client-Verbindungsanforderungen abhört. Es empfängt eingehende Client-Verbindungsanfragen und verwaltet den Datenverkehr dieser Anfragen an die Datenbank. Bevor Sie eine Verbindung zu einer Zieldatenbank oder einer Repository-Datenbankinstanz herstellen, können Sie mit dem STATUS-Befehl die Listener-Konfiguration überprüfen.

Der STATUS-Befehl zeigt grundlegende Statusinformationen zu einem bestimmten Listener an, einschließlich einer Zusammenfassung der Listener-Konfigurationseinstellungen, Listener-Protokolladressen und einer Zusammenfassung der bei diesem Listener registrierten Dienste.

1. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: 'Lsnrctl STATUS'

   Der dem Listener-Port zugewiesene Standardwert ist 1521.

SnapManager wird installiert

Sie müssen SnapManager auf jedem Host installieren, auf dem die Datenbank, die Sie sichern möchten, ausgeführt wird.

Sie müssen SnapDrive für UNIX auf dem Datenbank-Host installiert und eine Verbindung zum Speichersystem hergestellt haben.

Informationen zum Installieren SnapDrive und Herstellen einer Verbindung zum Storage-System finden Sie in der Dokumentation von SnapDrive für UNIX.

Sie müssen eine SnapManager-Instanz pro Datenbank-Host installieren. Wenn Sie eine RAC-Datenbank (Real Application Cluster) verwenden und die RAC-Datenbank sichern möchten, müssen Sie SnapManager auf allen Hosts der RAC-Datenbank installieren.

1. Laden Sie das SnapManager für Oracle Installationspaket für UNIX von der NetApp Support Site herunter und kopieren Sie es auf das Host-System.

   "NetApp Downloads: „Software""

2. Melden Sie sich beim Datenbank-Host als Root-Benutzer an.
3. Navigieren Sie in der Eingabeaufforderung zum Verzeichnis, in dem Sie das Installationspaket kopiert haben.
4. Machen Sie das Installationspaket ausführbar: Chmod 755install_package.bin

5. Installieren von SnapManager: './install_package.bin'
6. Drücken Sie die Eingabetaste, um fortzufahren.
7. Führen Sie folgende Schritte aus:

   a. Drücken Sie die Eingabetaste, um den Standardwert für die Betriebssystemgruppe zu übernehmen.

      Der Standardwert für die Gruppe ist dba.

   b. Drücken Sie die Eingabetaste, um den Standardwert für den Starttyp zu übernehmen.

   Die Konfigurationsübersicht wird angezeigt.

8. Überprüfen Sie die Konfigurationsübersicht, und drücken Sie die Eingabetaste, um fortzufahren.

   SnapManager ist installiert unter

Verwandte Informationen

Einrichtung von SnapManager

"NetApp Dokumentation: 'SnapDrive für UNIX'"

Einrichtung von SnapManager

Sie können SnapManager starten und entweder über die Benutzeroberfläche (UI) oder die Befehlszeilenschnittstelle (CLI) darauf zugreifen. Nach dem Zugriff auf SnapManager müssen Sie das SnapManager-Repository erstellen, bevor Sie SnapManager-Vorgänge durchführen.

Starten des SnapManager-Servers

Sie müssen den SnapManager-Server vom Ziel-Datenbank-Host starten.

1. Melden Sie sich beim Ziel-Datenbank-Host an und starten Sie den SnapManager-Server:

   Die folgende Meldung wird angezeigt: 'SnapManager-Server gestartet auf sicheren Port Port_number mit PID PID_number'.

   Der Standardport ist 27214.

Sie können überprüfen, ob SnapManager ordnungsgemäß ausgeführt wird:

Die folgende Meldung wird angezeigt: 'Operation ID Operation_ID_number erfolgreich.'

Zugriff auf die SnapManager Benutzeroberfläche

Sie können die SnapManager-Benutzeroberfläche (UI) Remote über einen Webbrowser von jedem System aus aufrufen, das auf einem von SnapManager unterstützten Betriebssystem ausgeführt wird. Sie können auch über den Ziel-Datenbank-Host auf die SnapManager-Benutzeroberfläche zugreifen, indem Sie den smogui-Befehl ausführen.

- Sie müssen sicherstellen, dass SnapManager ausgeführt wird.
- Sie müssen sicherstellen, dass das unterstützte Betriebssystem und Java auf dem System installiert sind, auf dem Sie auf die SnapManager-Benutzeroberfläche zugreifen möchten.

  Informationen zum unterstützten Betriebssystem und Java finden Sie im Interoperabilitäts-Matrix-Tool.

  a. Geben Sie im Webbrowser-Fenster Folgendes ein:https://server_name.domain.com:port_number[]
     - Server_Name ist der Name des Ziel-Datenbank-Hosts, auf dem SnapManager installiert ist.

       Sie können auch die IP-Adresse des Ziel-Datenbank-Hosts eingeben.

     - Port_number ist der Port, auf dem SnapManager ausgeführt wird.

       Der Standardwert ist 27214.

  b. Klicken Sie auf den Link.

     Die Benutzeroberfläche wird angezeigt.

SnapManager-Repository wird konfiguriert

Sie müssen das SnapManager-Repository in der Repository-Datenbankinstanz konfigurieren. Die Repository-Datenbank speichert Metadaten für Datenbanken, die von SnapManager gemanagt werden.

- Sie müssen die Repository-Datenbankinstanz erstellt haben.
- Sie müssen den Oracle-Benutzer für die Repository-Datenbankinstanz mit den erforderlichen Berechtigungen erstellt haben.
- Sie müssen die Details der Repository-Datenbankinstanz in die Datei nsnames.ora enthalten haben.

Sie können das SnapManager-Repository entweder über die SnapManager-Benutzeroberfläche (UI) oder über die Befehlszeilenschnittstelle (CLI) konfigurieren. Mit diesen Schritten wird das Erstellen eines Repositorys mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es bevorzugen.

Informationen zum Erstellen des Repositorys mithilfe von CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie im linken Bereich der SnapManager-Benutzeroberfläche mit der rechten Maustaste auf **Repositories**.
2. Wählen Sie **Neues Repository erstellen** und klicken Sie auf **Weiter**.
3. Geben Sie im Fenster Repository-Datenbankkonfigurationsinformationen die folgenden Informationen ein:

In diesem Feld…	Tun Sie das…
Benutzername	Geben Sie den Namen des Benutzers ein, den Sie für die Repository-Datenbankinstanz erstellt haben.
Passwort	Geben Sie das Passwort ein.

In diesem Feld…	Tun Sie das…
Gastgeber	Geben Sie die IP-Adresse des Hosts ein, auf dem die Repository-Datenbankinstanz erstellt wird.
Port	Geben Sie den Port ein, der für die Verbindung zur Repository-Datenbankinstanz verwendet wird. Der Standardport ist 1521.
Dienstname	Geben Sie den Namen ein, den SnapManager für die Verbindung zur Repository-Datenbankinstanz verwendet. Je nach den Details in der Datei nsnames.ora kann es sich um den kurzen Servicenamen oder den vollqualifizierten Servicenamen handelt. +

4. Überprüfen Sie im Fenster Projektarchiv hinzufügen die Konfigurationszusammenfassung und klicken Sie auf **Hinzufügen**.

   Wenn der Vorgang fehlschlägt, klicken Sie auf die Registerkarte **Operationsinformationen**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat. Die Fehlerdetails werden auch im Betriebsprotokoll unter /var/log/smo erfasst.

5. Klicken Sie Auf **Fertig Stellen**.

   Das Repository wird im linken Fensterbereich unter dem Baum **Repositories** aufgelistet. Wenn das Repository nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf **Repositories** und klicken Sie auf **Aktualisieren**.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Sichern und Überprüfen Ihrer Datenbanken

Nach der Installation von SnapManager können Sie ein Basis-Backup Ihrer Datenbank erstellen und überprüfen, ob das Backup keine beschädigten Dateien enthält.

Verwandte Informationen

SnapManager Backup – Überblick

Backup-Strategie definieren

Erstellen eines Profils für Ihre Datenbank

Sichern Ihrer Datenbank

Datenbank-Backups werden überprüft

SnapManager Backup – Überblick

SnapManager erstellt mithilfe von NetApp Snapshot Technologie die Backups von Datenbanken. Sie können das DBVERIFY-Dienstprogramm verwenden oder SnapManager verwenden, um die Integrität der Backups zu überprüfen.

SnapManager sichert eine Datenbank, indem Snapshot Kopien der Volumes erstellt werden, die Datendateien, Kontrolldateien und Archivprotokolldateien enthalten. Diese Snapshot Kopien bestehen zusammen aus einem Backup-Set, mit dem SnapManager eine Datenbank wiederherstellen kann.

Backup-Strategie definieren

Wenn Sie eine Backup-Strategie vor der Erstellung Ihrer Backups definieren, stellen Sie sicher, dass Ihnen Backups zur erfolgreichen Wiederherstellung Ihrer Datenbanken zur Verfügung stehen. SnapManager bietet einen flexiblen, granularen Backup-Zeitplan, der Ihr Service Level Agreement (SLA) erfüllt.

Informationen zu den Best Practices für SnapManager finden Sie unter *TR 3761*.

Welcher Modus für SnapManager Backups benötigen Sie?

SnapManager unterstützt zwei Backup-Modi:

Backup-Modus	Beschreibung
Online-Backup	Erstellt ein Backup der Datenbank, wenn sich die Datenbank im Online-Status befindet. Dieser Backup-Modus wird auch als Hot Backup bezeichnet.
Offline-Backup	Erstellt eine Sicherung der Datenbank, wenn sich die Datenbank entweder im angehängten oder abschaltenden Zustand befindet. Dieser Backup-Modus wird auch als Cold Backup bezeichnet.

Welche Art von SnapManager-Backup benötigen Sie?

SnapManager unterstützt drei Arten von Backups:

Backup-Typ	Beschreibung
Vollständiges Backup	Erstellt ein Backup der gesamten Datenbank, die alle Datendateien, Kontrolldateien und Archivprotokolldateien umfasst.
Teilweise Sicherung	Erstellt ein Backup ausgewählter Datendateien, Kontrolldateien, Tablespaces und Archivprotokolldateien

Backup-Typ	Beschreibung
Backup nur für Archivierung	Erstellt eine Sicherung nur der Archivprotokolldateien.Sie müssen beim Erstellen des Profils **Archivprotokolle separat** auswählen.

Was für ein Datenbankprofil benötigen Sie?

SnapManager erstellt Backups basierend darauf, ob das Datenbankprofil die Archiv-Log-Backups von den Datendatei-Backups trennt.

Profiltyp	Beschreibung
Ein einzelnes Datenbankprofil für eine kombinierte Sicherung von Datendateien und Archivprotokollen	Ermöglicht Ihnen das Erstellen von: • Vollständige Sicherung mit allen Datendateien, Archivprotokolldateien und Kontrolldateien • Partielles Backup mit ausgewählten Datendateien, Tablespaces, Archivprotokolldateien und Kontrolldateien
Separate Datenbankprofile für Backups von Archivierungsprotokolldaten und Datendatei-Backups	Ermöglicht Ihnen das Erstellen von: • Kombiniertes Backup mit unterschiedlichen Kennungen für Backup von Datendateien und Backup von Archivierungsprotokolldaten • Datendatei-only-Backup aller Datendateien zusammen mit den Kontrolldateien • Partielles, datenonly Backup von ausgewählten Datendateien oder Tablespaces zusammen mit den Control Files • Backup nur bei Archivierung und Protokollen

Welche Namenskonventionen sollten für Snapshot Kopien verwendet werden?

Von Backups erstellte Snapshot Kopien können einer benutzerdefinierten Namenskonvention folgen. Benutzerdefinierte Text oder integrierte Variablen wie der Profilname, der Datenbankname und die von SnapManager bereitgestellte Datenbank-SID können zur Erstellung der Namenskonvention verwendet werden. Sie können die Namenskonvention erstellen, während Sie die Richtlinie erstellen.

Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

Die Namenskonventionen für Snapshot Kopien können während oder nach der Erstellung eines Profils geändert werden. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Vorhandene Snapshot Kopien behalten das vorherige Muster bei.

Wie lange möchten Sie Backup-Kopien auf dem primären Storage-System und dem sekundären Storage-System aufbewahren?

In einer Backup-Aufbewahrungsrichtlinie wird die Anzahl der erfolgreichen Sicherungskopien festgelegt, die aufbewahrt werden sollen. Sie können die Aufbewahrungsrichtlinie angeben, während Sie die Richtlinie erstellen.

Sie können stündlich, täglich, wöchentlich, monatlich oder unbegrenzt als Aufbewahrungsklasse auswählen. Sie können für jede Aufbewahrungsklasse den Aufbewahrungszähler und die Aufbewahrungsdauer entweder gemeinsam oder einzeln festlegen.

- Die Anzahl der Aufbewahrung bestimmt die Mindestanzahl der Backups einer bestimmten Aufbewahrungsklasse, die beibehalten werden soll.

  Wenn beispielsweise der Backup-Zeitplan *Daily* lautet und die Anzahl der Aufbewahrung *10* ist, werden 10 tägliche Backups aufbewahrt.

  Die maximale Anzahl von Snapshot Kopien, die Sie mit Data ONTAP aufbewahren können, ist 255. Nach Erreichen des maximalen Limits schlägt die Erstellung neuer Snapshot Kopien standardmäßig fehl. Sie können jedoch die Rotationsrichtlinie in Data ONTAP konfigurieren, um ältere Snapshot-Kopien zu löschen.

- Die Aufbewahrungsdauer legt die Mindestanzahl an Tagen fest, für die das Backup aufbewahrt werden soll.

  Wenn beispielsweise der Backup-Zeitplan *täglich* lautet und die Aufbewahrungsdauer *10* beträgt, werden täglich 10 Tage Backups aufbewahrt.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

Zur langfristigen Aufbewahrung von Backup-Kopien sollten Sie SnapVault verwenden.

Möchten Sie Backup-Kopien mithilfe des Quell-Volume oder eines Ziel-Volume überprüfen?

Wenn Sie SnapMirror oder SnapVault einsetzen, können Sie Backup-Kopien mithilfe der Snapshot-Kopie auf dem SnapMirror oder SnapVault Ziel-Volume überprüfen anstelle der Snapshot-Kopie auf dem primären Storage-System. Die Verwendung eines Ziel-Volumes zur Verifizierung reduziert die Last auf dem primären Storage-System.

Verwandte Informationen

"Technischer Bericht 3761: SnapManager für Oracle: Best Practices"

Erstellen eines Profils für Ihre Datenbank

Sie müssen ein Profil erstellen, damit Ihre Datenbank alle Vorgänge in dieser Datenbank ausführen kann. Das Profil enthält Informationen über die Datenbank und kann nur auf eine Datenbank verweisen. Eine Datenbank kann jedoch durch mehrere Profile referenziert werden. Ein Backup, das mit einem Profil erstellt wird, kann nicht von einem anderen Profil aus aufgerufen werden, auch wenn beide Profile mit derselben Datenbank verknüpft sind.

Sie müssen sicherstellen, dass die Details der Zieldatenbank in der Datei /etc/oratab enthalten sind.

Mit diesen Schritten wird die Erstellung eines Profils für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche erläutert. Sie können auch die CLI verwenden, wenn Sie es bevorzugen.

Informationen zum Erstellen von Profilen mithilfe der CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie in der Repository-Struktur mit der rechten Maustaste auf das Repository oder den Host und wählen Sie **Profil erstellen** aus.
2. Geben Sie auf der Seite Profilkonfigurationsinformationen den benutzerdefinierten Namen und das Kennwort für das Profil ein.
3. Geben Sie auf der Seite Datenbankkonfigurationsinformationen die folgenden Informationen ein:

In diesem Feld…	Tun Sie das…
Datenbankname	Geben Sie den Namen der Datenbank ein, die Sie sichern möchten.
• Datenbank-SID*	Geben Sie die sichere ID (SID) der Datenbank ein. Der Datenbankname und die Datenbank-SID können identisch sein.
Gastgeber	Geben Sie die IP-Adresse des Hosts ein, auf dem sich die Zieldatenbank befindet. Sie können auch den Hostnamen angeben, wenn der Hostname im Domain Name System (DNS) angegeben ist.
Host-Konto	Geben Sie den Oracle-Benutzernamen der Zieldatenbank ein. der Standardwert für den Benutzer ist oracle.
Host-Gruppe	Geben Sie den Namen der Oracle-Benutzergruppe ein. Der Standardwert ist dba. +

4. Wählen Sie auf der Seite Datenbankverbindungsinformationen eine der folgenden Optionen aus:

Wählen Sie diese Option…	Ihr Ziel ist
O/S-Authentifizierung verwenden	Verwenden Sie die vom Betriebssystem gepflegten Anmeldeinformationen, um Benutzer zu authentifizieren, die auf die Datenbank zugreifen.

Wählen Sie diese Option…	Ihr Ziel ist
Datenbankauthentifizierung Verwenden	Erlauben Sie Oracle, einen administrativen Benutzer mithilfe der Authentifizierung von Kennwortdateien zu authentifizieren. Geben Sie die entsprechenden Informationen zur Datenbankverbindung ein. • Geben Sie im Feld **SYSDBA Privileged User Name** den Namen des Datenbankadministrators mit Administratorrechten ein. • Geben Sie im Feld **Passwort** das Passwort des Datenbankadministrators ein. • Geben Sie im Feld **Port** die Portnummer ein, die für die Verbindung mit dem Host verwendet wird, auf dem sich die Datenbank befindet. Der Standardwert ist .
Verwendung der ASM-Instanz-Authentifizierung	Zulassen, dass die ASM-Datenbankinstanz einen administrativen Benutzer authentifiziert. Geben Sie die entsprechenden Authentifizierungsdaten für die ASM-Instanz ein. • Geben Sie im Feld **SYSDBA/SYSASM Privileged User Name** den Benutzernamen des ASM-Instanzadministrators mit Administratorrechten ein. • Geben Sie im Feld **Passwort** das Passwort des Administrators ein.

Hinweis: Sie können den ASM-Authentifizierungsmodus nur auswählen, wenn Sie eine ASM-Instanz auf dem Datenbank-Host haben.

5. Wählen Sie auf der Seite RMAN-Konfigurationsinformationen eine der folgenden Optionen aus:

Wählen Sie diese Option…	Wenn…
Verwenden Sie nicht RMAN	Sie verwenden RMAN nicht für das Management von Backup- und Restore-Vorgängen.
Verwenden Sie RMAN über die Steuerdatei	Sie verwalten das RMAN-Repository mit Steuerdateien.

Wählen Sie diese Option…	Wenn…
Verwenden Sie RMAN über den Wiederherstellungskatalog	Sie verwalten das RMAN-Repository mithilfe der Recovery-Katalogdatenbank. Geben Sie den Benutzernamen ein, der Zugriff auf die Datenbank des Wiederherstellungspatalogs, das Kennwort und den Oracle-Nettodienstnamen der Datenbank hat, die die TNS-Verbindung (Transparent Network Substrat) verwaltet. +

6. Wählen Sie auf der Seite Snapshot Naming Information die Variablen aus, um ein Benennungsformat für die Snapshot Kopie anzugeben.

   Sie müssen die smid-Variable in das Benennungsformat aufnehmen. Die smid-Variable erstellt eine eindeutige Snapshot-Kennung.

7. Führen Sie auf der Seite Richtlinieneinstellungen folgende Schritte durch:
   a. Geben Sie Anzahl und Dauer der Aufbewahrung für jede Aufbewahrungsklasse ein.
   b. Wählen Sie aus der Dropdown-Liste **Protection Policy** die Protection Manager-Richtlinie aus.
   c. Wenn Sie Archivprotokolle separat sichern möchten, aktivieren Sie das Kontrollkästchen **Archivprotokolle separat sichern**, legen Sie die Aufbewahrung fest und wählen Sie die Schutzrichtlinie aus.

      Sie können eine Richtlinie auswählen, die sich von der für Datendateien verknüpften Richtlinie unterscheidet. Wenn Sie beispielsweise eine der Protection Manager-Richtlinie für Datendateien ausgewählt haben, können Sie eine andere Protection Manager-Richtlinie für Archivprotokolle auswählen.

8. Geben Sie auf der Seite Benachrichtigungseinstellungen konfigurieren die Einstellungen für E-Mail-Benachrichtigungen an.
9. Wählen Sie auf der Seite Verlaufsdaten-Konfigurationsinformationen eine der Optionen aus, um den Verlauf der SnapManager-Vorgänge beizubehalten.
10. Überprüfen Sie auf der Seite Vorgang „Profil erstellen“ die Informationen und klicken Sie auf **Erstellen**.
11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

    Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Sichern Ihrer Datenbank

Nachdem Sie ein Profil erstellt haben, müssen Sie Ihre Datenbank sichern. Sie können wiederkehrende Backups nach der erstmaligen Sicherung und Überprüfung planen.

In diesen Schritten wird gezeigt, wie Sie mithilfe der SnapManager-Benutzeroberfläche ein Backup Ihrer

Datenbank erstellen. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden.

Informationen zur Erstellung von Backups mit CLI finden Sie im *SnapManager for Oracle Administration Guide for UNIX*.

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die zu sicherende Datenbank enthält, und wählen Sie **Backup** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

   Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

   Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die override.default.backup.pattern und new.default.backup.pattern Konfigurationsvariablen bearbeiten, um Ihr eigenes Standard-Backup-Label-Muster zu erstellen.

3. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

   Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

4. Führen Sie auf der Seite Datenbank, Tablespaces oder Datendateien zur Datensicherung die folgenden Schritte aus:
   a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
   b. Wählen Sie **Backup Archivelogs** aus, um die Archiv-Log-Dateien separat zu sichern.
   c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.

      Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

   d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

      Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

   e. Wählen Sie **Jetzt schützen** aus, wenn Sie die Sicherung sofort auf dem sekundären Speicher schützen möchten, der den Schutzzeitplan des Protection Manager überschreibt.
   f. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

      Wenn Sie Auto auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

   g. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
   h. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.
5. Geben Sie auf der Seite Task Enabling an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.

6. Überprüfen Sie auf der Seite Backup-Vorgang durchführen die Informationen und klicken Sie auf **Backup**.
7. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

   Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Datenbank-Backups werden überprüft

Sie können die Sicherung Ihrer Datenbank überprüfen, um sicherzustellen, dass die gesicherten Dateien nicht beschädigt sind.

Wenn Sie beim Erstellen eines Backups nicht das Kontrollkästchen **Backup überprüfen mit dem Dienstprogramm Oracle DBVERIFY** aktiviert haben, müssen Sie diese Schritte manuell durchführen, um die Sicherung zu überprüfen. Wenn Sie das Kontrollkästchen aktiviert haben, überprüft SnapManager das Backup automatisch.

1. Wählen Sie aus der Struktur **Repositories** das Profil aus.
2. Klicken Sie mit der rechten Maustaste auf das Backup, das Sie überprüfen möchten, und wählen Sie **Überprüfen**.
3. Klicken Sie Auf **Fertig Stellen**.

   Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

   Klicken Sie im Baum **Repository** mit der rechten Maustaste auf das Backup und klicken Sie dann auf **Eigenschaften**, um die Ergebnisse des Verifizierungsvorgangs anzuzeigen.

Sie können gesicherte Dateien verwenden, um Wiederherstellungsvorgänge durchzuführen. Informationen zur Durchführung von Wiederherstellungsvorgängen über die SnapManager-Benutzeroberfläche (UI) finden Sie in der *Online-Hilfe*. Wenn Sie die Befehlszeilenschnittstelle (CLI) zum Durchführen von Wiederherstellungsvorgängen verwenden möchten, finden Sie im *SnapManager für Oracle – Administratorhandbuch für UNIX*.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Planung wiederkehrender Backups

Sie können Backup-Vorgänge so planen, dass die Backups automatisch in regelmäßigen Abständen initiiert werden. SnapManager ermöglicht die Planung von Backups auf Stundenbasis, täglich, wöchentlich, monatlich oder einmalig.

Sie können mehrere Backup-Zeitpläne für eine einzige Datenbank zuweisen. Wenn Sie jedoch mehrere Backups für dieselbe Datenbank planen, müssen Sie sicherstellen, dass die Backups nicht gleichzeitig geplant sind.

Mit diesen Schritten wird das Erstellen eines Backup-Zeitplans für Ihre Datenbank mithilfe der SnapManager-Benutzeroberfläche (UI) erläutert. Falls Sie möchten, können Sie auch die Befehlszeilenschnittstelle (CLI) verwenden. Informationen zum Planen von Backups mithilfe der CLI finden Sie im Administratorhandbuch „*SnapManager für Oracle Administration Guide for UNIX*“.

1. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf das Profil, das die Datenbank enthält, für die Sie einen Backup-Zeitplan erstellen möchten, und wählen Sie **Backup planen** aus.
2. Geben Sie unter **Label** einen benutzerdefinierten Namen für das Backup ein.

   Sie dürfen keine Leerzeichen oder Sonderzeichen in den Namen einfügen. Wenn Sie keinen Namen angeben, erstellt SnapManager automatisch eine Sicherungsbezeichnung.

   Ab SnapManager 3.4 können Sie das von SnapManager erstellte Backup-Label ändern. Sie können die Variablen override.default.backup.pattern und new.default.backup.patternconfiguration bearbeiten, um Ihr eigenes Standard-Backup-Label-Muster zu erstellen.

3. Wählen Sie **Starten oder Herunterfahren der Datenbank zulassen, falls erforderlich**, um den Status der Datenbank zu ändern, falls erforderlich.

   Diese Option stellt sicher, dass, wenn sich die Datenbank nicht im erforderlichen Zustand befindet, um ein Backup zu erstellen, SnapManager die Datenbank automatisch in den gewünschten Zustand bringt, um den Vorgang abzuschließen.

4. Führen Sie auf der Seite Datenbank, Tablespaces oder Datendateien zur Datensicherung die folgenden Schritte aus:
   a. Wählen Sie **Datendateien sichern** aus, um entweder die komplette Datenbank, ausgewählte Datendateien oder ausgewählte Tabellen zu sichern.
   b. Wählen Sie **Backup Archivelogs** aus, um die Archiv-Log-Dateien separat zu sichern.
   c. Wählen Sie **Prune Archivelogs** aus, wenn Sie die Archiv-Log-Dateien aus dem aktiven Dateisystem löschen möchten, das bereits gesichert ist.

      Wenn Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist, dann kann SnapManager die Archiv-Log-Dateien nicht beschneiden.

   d. Wählen Sie **Sichern Sie das Backup**, wenn Sie den Backup-Schutz aktivieren möchten.

      Diese Option ist nur aktiviert, wenn die Schutzrichtlinie beim Erstellen des Profils ausgewählt wurde.

   e. Wählen Sie **Jetzt schützen** aus, wenn Sie die Sicherung sofort auf dem sekundären Speicher schützen möchten, der den Schutzzeitplan des Protection Manager überschreibt.
   f. Wählen Sie aus der Dropdown-Liste **Typ** den Backup-Typ (offline oder online) aus, den Sie erstellen möchten.

      Wenn Sie Auto auswählen, erstellt SnapManager basierend auf dem aktuellen Status der Datenbank ein Backup.

   g. Wählen Sie aus der Dropdown-Liste **Retention Class** die Aufbewahrungsklasse aus.
   h. Aktivieren Sie das Kontrollkästchen **Backup überprüfen mit dem Oracle DBVERIFY Utility**, wenn Sie sicherstellen möchten, dass die gesicherten Dateien nicht beschädigt sind.
5. Geben Sie im Feld **Terminplanname** einen benutzerdefinierten Namen des Zeitplans ein.

   Sie dürfen keine Leerzeichen in den Namen einfügen.

6. Führen Sie auf der Seite Backup Schedule konfigurieren die folgenden Schritte aus:
   a. Wählen Sie aus der Dropdown-Liste **Durchführung dieser Operation** die Häufigkeit des Backup-

Zeitplans aus.

b. Geben Sie im Feld **Startdatum** das Datum an, an dem Sie den Backup-Zeitplan starten möchten.

c. Geben Sie im Feld **Startzeit** den Zeitpunkt an, zu dem der Backup-Zeitplan gestartet werden soll.

d. Geben Sie das Intervall an, in dem Backups erstellt werden sollen.

   Wenn Sie beispielsweise die Frequenz als stündlich ausgewählt haben und das Intervall als 2 angeben, werden die Backups alle 2 Stunden geplant.

7. Geben Sie auf der Seite Task Enabling an, ob Sie Aufgaben vor und nach Abschluss der Backup-Vorgänge ausführen möchten.
8. Überprüfen Sie auf der Seite Backup Schedule Operation durchführen die Informationen und klicken Sie auf **Zeitplan**.
9. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

   Wenn der Vorgang fehlschlägt, klicken Sie auf **Betriebsdetails**, um anzuzeigen, was den Vorgang zum Scheitern verurteilt hat.

Verwandte Informationen

"SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

Weitere Schritte

Nach der Installation von SnapManager und dem erfolgreichen Erstellen eines Backups können Sie mit SnapManager Wiederherstellungs-, Recovery- und Klonvorgänge durchführen. Zusätzlich erhalten Sie eventuell Informationen zu anderen SnapManager Funktionen, wie zum Beispiel Planung, Management des SnapManager Betriebs und Aufrechterhaltung der Historie von Aktivitäten.

Weitere Informationen zu diesen Funktionen sowie Informationen zur Version von SnapManager finden Sie in der folgenden Dokumentation. Alle Informationen finden Sie im "NetApp Support".

- "SnapManager 3.4 für Oracle – Administratorhandbuch für UNIX"

  Beschreibt die Konfiguration und Verwaltung von SnapManager für Oracle. Die Themen umfassen das Konfigurieren, Sichern, Wiederherstellen und Klonen von Datenbanken, das Durchführen von Sekundärschutz, Außerdem eine Erläuterung der CLI-Befehle und Anweisungen zum Upgrade und der Deinstallation des Produkts.

- "Versionshinweise zu SnapManager 3.4 für Oracle"

  Beschreibt neue Funktionen, feste Probleme, wichtige Vorsichtsmaßnahmen, bekannte Probleme und Einschränkungen für SnapManager für Oracle.

- *SnapManager für Oracle Online-Hilfe*

  Beschreibt die Schritt-für-Schritt-Verfahren zur Durchführung verschiedener SnapManager-Vorgänge mithilfe der SnapManager-Benutzeroberfläche.

Die *Online-Hilfe* ist in die SnapManager-Benutzeroberfläche integriert und steht nicht auf der Support-Website zur Verfügung.

- "Technischer Bericht 3761: SnapManager für Oracle: Best Practices"

  Beschreibt die Best Practices von SnapManager für Oracle.

- "NetApp Technical Report 3633: Best Practices for Oracle Databases on NetApp Storage"

  Beschreibt Best Practices zur Konfiguration von Oracle Datenbanken auf NetApp Storage-Systemen.

Verwandte Informationen

"NetApp Support"

"NetApp Dokumentation: Produktbibliothek A-Z"

Administrationshandbuch für UNIX®

Dieser Leitfaden beschreibt die Administration von SnapManager 3.4.2 für Oracle in einer UNIX-Umgebung nach Abschluss der Bereitstellung. Er enthält Informationen zur Konfiguration, Aktualisierung und Deinstallation des Produkts, zur Sicherung, Wiederherstellung und zum Klonen von Datenbanken.

Produktübersicht

SnapManager für Oracle automatisiert und vereinfacht komplexe, manuelle und zeitintensive Prozesse, die im Zusammenhang mit Backup, Recovery und Klonen von Oracle Datenbanken anfallen. Mithilfe von SnapManager mit ONTAP SnapMirror Technologie können Sie Backup-Kopien auf einem anderen Volume erstellen. Mit der ONTAP SnapVault Technologie werden Backups effizient auf Festplatten archiviert.

SnapManager lässt sich mit nativen Oracle Technologien wie Oracle Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) und Direct NFS über FC-, iSCSI- und NFS-Protokolle integrieren. Optional können mit SnapManager erstellte Backups mit dem Oracle Recovery Manager (RMAN) katalogisiert werden, um die Backup-Informationen zu erhalten. Diese Backups können später in Restore-Vorgängen auf Blockebene oder in zeitpunktgenauen Recovery-Vorgängen verwendet werden.

SnapManager Highlights

SnapManager ermöglicht die nahtlose Integration mit Oracle Datenbanken auf dem UNIX Host und über das Backend mit NetApp Snapshot, SnapRestore und FlexClone Technologien Es bietet eine benutzerfreundliche Oberfläche (UI) und eine Befehlszeilenschnittstelle (CLI) für Administrationsfunktionen.

Mit SnapManager können Sie folgende Datenbankvorgänge ausführen und Daten effizient managen:

- Erstellung platzsparender Backups auf primärem oder sekundärem Storage

  Sie können die Datendateien und Protokolldateien separat archivieren.

- Planen von Backups
- Wiederherstellung von vollständigen oder teilweisen Datenbanken unter Verwendung eines dateibasierten oder Volume-basierten Restore-Vorgangs
- Wiederherstellung von Datenbanken durch Erkennung, Mounten und Anwendung von Archivprotokolldateien aus Backups
- Beschneiden von Archiv-Log-Dateien von Archiv-Protokollzielen bei der Erstellung von Backups nur der Archivprotokolle
- Automatische Aufbewahrung einer minimalen Anzahl von Archiv-Log-Backups, da nur die Backups gespeichert werden, die eindeutige Archivprotokolldateien enthalten
- Verfolgung von Betriebsdetails und Erstellung von Berichten
- Backup wird überprüft, um sicherzustellen, dass sich Backups in einem gültigen Blockformat befinden und dass keine der gesicherten Dateien beschädigt sind
- Pflegen eines Verlaufs von Vorgängen, die im Datenbankprofil durchgeführt werden

  Ein Profil enthält Informationen über die Datenbank, die von SnapManager gemanagt werden soll.

- Erstellung platzsparender Backup-Klone auf primären oder sekundären Storage-Systemen

  SnapManager ermöglicht Ihnen die Aufteilung eines Datenbankklonen.

Backups mit Snapshot Kopien erstellen

Mit SnapManager können Sie Backups auf dem primären (lokalen) Storage und auch auf dem sekundären (Remote-) Storage mithilfe von Sicherungsrichtlinien oder Nachbearbeitungsskripten erstellen.

Als Snapshot-Kopien erstellte Backups sind virtuelle Kopien der Datenbank und werden auf demselben physischen Medium wie die Datenbank gespeichert. Der Backup-Vorgang dauert daher weniger Zeit und erfordert deutlich weniger Speicherplatz als vollständige Disk-to-Disk Backups. Mit SnapManager können Sie Folgendes sichern:

- Alle Datendateien, archivierte Log-Dateien und Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces, alle Archivprotokolldateien und Kontrolldateien

Mit SnapManager 3.2 oder höher können Sie optional folgende Daten sichern:

- Alle Datendateien und die Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces zusammen mit den Kontrolldateien
- Archivierung von Protokolldateien

> Die Datendateien, Archiv-Log-Dateien und Kontrolldateien können auf verschiedenen Storage-Systemen, Storage-System-Volumes oder LUNs (Logical Unit Numbers) abgelegt werden. Sie können SnapManager auch zum Backup einer Datenbank verwenden, wenn sich mehrere Datenbanken auf demselben Volume oder LUN befinden.

Warum sollten Sie Archiv Log-Dateien beschneiden

Mit SnapManager für Oracle können Sie Archivprotokolldateien aus dem aktiven, bereits gesicherten Dateisystem löschen.

Durch Beschneidung kann SnapManager Backups einzelner Archiv-Log-Dateien erstellen. Durch Beschneidung und die Richtlinie zur Aufbewahrung von Backups wird beim Säuberen von Backups der Speicherplatz für das Archiv-Protokoll freigegeben.

> Sie können die Archivprotokolldateien nicht beschneiden, wenn der Flash Recovery Area (FRA) für Archivprotokolldateien aktiviert ist. Wenn Sie im Bereich Flash Recovery den Speicherort für das Archivprotokoll angeben, müssen Sie im Parameter Archive_log_dest auch den Speicherort für das Archivprotokoll angeben.

Konsolidierung von Archivierungsprotokolldaten

Mit SnapManager (3.2 oder höher) für Oracle werden die Archiv-Log-Backups konsolidiert, um eine Mindestanzahl an Backups für Archivierungs-Log-Dateien beizubehalten. SnapManager für Oracle erkennt und befreit die Backups, die Archivprotokolle enthalten, die Teilmengen anderer Backups sind.

Vollständige oder teilweise Wiederherstellung von Datenbanken

SnapManager bietet die Flexibilität, komplette Datenbanken, bestimmte Tabellen, Dateien, Kontrolldateien oder eine Kombination dieser Einheiten wiederherzustellen. SnapManager ermöglicht die Wiederherstellung von Daten mithilfe eines dateibasierten Wiederherstellungsprozesses mit einem schnelleren, Volume-basierten Wiederherstellungsprozess. Datenbankadministratoren können den Prozess auswählen, den sie verwenden möchten, oder SnapManager entscheiden lassen, welcher Prozess für Sie geeignet ist.

SnapManager ermöglicht Datenbankadministratoren (DBAs) die Vorschau von Restore-Vorgängen. Mit der Vorschaufunktion können DBAs jeden Wiederherstellungsvorgang auf Datei-für-Datei-Basis anzeigen.

Datenbankadministratoren können das Level angeben, auf das SnapManager bei der Durchführung von Restore-Vorgängen wiederhergestellt und Informationen wiederhergestellt werden. Beispielsweise können DBAs Daten zu bestimmten Zeitpunkten wiederherstellen. Der Wiederherstellungspunkt kann ein Datum und eine Uhrzeit oder eine Oracle System Change Number (SCN) sein.

Datenbankadministratoren können die Datenbank mit SnapManager wiederherstellen und ein anderes Tool verwenden, um die Informationen wiederherzustellen. DBAs müssen für beide Vorgänge keine SnapManager verwenden.

Mit SnapManager (3.2 oder höher) können Datenbank-Backups automatisch und ohne Eingriff des Datenbankadministrators wiederhergestellt werden. Sie können SnapManager verwenden, um Backups für Archivprotokolle zu erstellen und dann diese Backups für Archivprotokolle zu verwenden, um die Datenbank-Backups wiederherzustellen und wiederherzustellen. Selbst wenn die Archivprotokolldateien des Backups in einem externen Archivprotokoll verwaltet werden, können Sie diesen externen Speicherort angeben, damit diese Archivprotokolle zur Wiederherstellung der wiederhergestellten Datenbank beitragen können.

Überprüfen des Backup-Status

SnapManager kann die Integrität des Backups mithilfe von standardmäßigen Oracle-Backup-Verifizierungsvorgängen bestätigen.

Datenbankadministratoren (DBAs) können die Verifizierung im Rahmen des Backup-Vorgangs oder einer anderen Zeit durchführen. Datenbankadministratoren können den Verifizierungsvorgang so einstellen, dass er bei geringerer Auslastung des Host-Servers oder während eines geplanten Wartungsfensters ausgeführt wird.

Datenbank-Backup-Klone

SnapManager erstellt mithilfe der FlexClone Technologie einen beschreibbaren, platzsparenden Klon eines Datenbank-Backups. Sie können einen Klon ändern, ohne die Backup-Quelle zu ändern.

Möglicherweise möchten Sie Datenbanken klonen, um Tests oder Upgrades in nicht produktiven Umgebungen zu ermöglichen. Sie können eine Datenbank mit einem primären oder sekundären Storage klonen. Ein Klon kann sich auf demselben Host oder einem anderen Host befinden wie die Datenbank.

Mit der FlexClone Technologie können SnapManager Snapshot-Kopien der Datenbank verwenden, sodass keine vollständige physische Disk-to-Disk-Kopie erstellt werden muss. Snapshot Kopien benötigen weniger Erstellungszeit und belegen deutlich weniger Speicherplatz als physische Kopien.

In der Data ONTAP Dokumentation finden Sie weitere Informationen zur FlexClone Technologie.

Verwandte Informationen

"Data ONTAP documentation: mysupport.netapp.com/documentation/productsatoz/index.html"

Verfolgen Sie die Details und erstellen Sie Berichte

SnapManager bietet nicht nur detaillierte Datenbankadministratoren, die den Status verschiedener Vorgänge verfolgen müssen, sondern mithilfe von Methoden, die Vorgänge über eine einheitliche Benutzeroberfläche überwachen.

Nachdem Administratoren festlegen, welche Datenbanken gesichert werden sollen, identifiziert SnapManager die Datenbankdateien für das Backup automatisch. SnapManager zeigt Informationen zu Repositorys, Hosts, Profilen, Backups und Klonen an. Sie können die Vorgänge auf bestimmten Hosts oder Datenbanken überwachen.Sie können auch die geschützten Backups identifizieren und bestimmen, ob die Backups in Bearbeitung sind oder geplant werden.

Repositories

SnapManager organisiert die Informationen in Profile, die dann den Repositories zugeordnet werden. Profile enthalten Informationen über die zu verwaltende Datenbank, während das Repository Daten zu den Vorgängen enthält, die auf Profilen ausgeführt werden.

Das Repository zeichnet auf, wann ein Backup durchgeführt wurde, welche Dateien gesichert wurden und ob ein Klon aus dem Backup erstellt wurde. Wenn Datenbankadministratoren eine Datenbank wiederherstellen oder einen Teil davon wiederherstellen, fragt SnapManager das Repository ab, um zu ermitteln, was gesichert wurde.

Da das Repository die Namen der während des Backup erstellten Datenbank-Snapshot-Kopien speichert, kann die Repository-Datenbank nicht in derselben Datenbank vorhanden sein und kann auch nicht Teil derselben Datenbank sein, die von SnapManager gesichert wird. Sie müssen mindestens zwei Datenbanken (die SnapManager Repository-Datenbank und die von SnapManager gemanagte Zieldatenbank) einrichten und ausführen, wenn Sie SnapManager Vorgänge ausführen.

Wenn Sie versuchen, die grafische Benutzeroberfläche (GUI) zu öffnen, wenn die Repository-Datenbank nicht verfügbar ist, wird die folgende Fehlermeldung in der Datei sm_gui.log protokolliert: [WARNUNG]: SMO-01106: Beim Abfragen des Repository ist ein Fehler aufgetreten: Keine Daten mehr aus dem Socket zu lesen. Außerdem schlägt das SnapManager-Verfahren fehl, wenn die Repository-Datenbank ausfällt. Weitere Informationen zu den verschiedenen Fehlermeldungen finden Sie unter *Fehlerbehebung bekannter Probleme*.

Sie können jeden beliebigen Host-Namen, Dienstnamen oder Benutzernamen verwenden, um Vorgänge auszuführen. Damit ein Repository SnapManager-Vorgänge unterstützt, müssen der Projektarchiv-Benutzername und der Dienstname nur aus den folgenden Zeichen bestehen: Alphabetische Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-), Unterstrich (_) und Punkt (.).

Der Repository-Port kann eine beliebige gültige Portnummer sein, und der Repository-Hostname kann einen beliebigen gültigen Hostnamen sein. Der Hostname muss aus alphabetischen Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-) und Periode (.) bestehen, jedoch nicht aus einem Unterstrich (_).

Das Repository muss in einer Oracle-Datenbank erstellt werden. Die von SnapManager verwendete Datenbank sollte gemäß den Oracle Verfahren für die Datenbankkonfiguration eingerichtet werden.

Ein einziges Repository kann Informationen über mehrere Profile enthalten, jedoch ist jede Datenbank normalerweise nur mit einem Profil verknüpft. Sie können mehrere Repositorys haben, wobei jedes Repository mehrere Profile enthält.

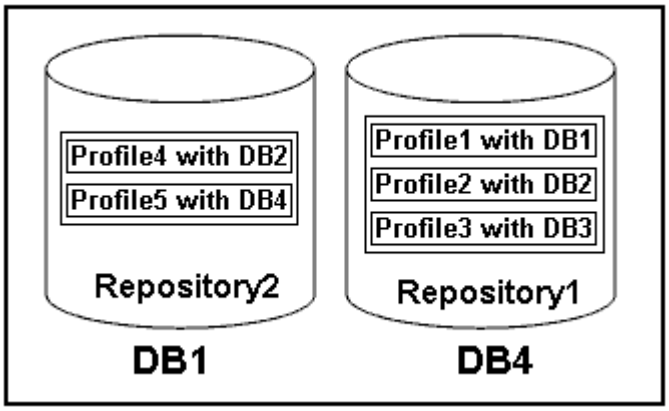
Welche Profile sind

SnapManager verwendet Profile, um die zur Durchführung von Operationen in einer bestimmten Datenbank erforderlichen Informationen zu speichern. Ein Profil enthält die Informationen zur Datenbank einschließlich aller Anmeldeinformationen, Backups und Klone. Wenn Sie ein Profil erstellen, müssen Sie keine Datenbankdetails angeben, wenn Sie eine Operation in dieser Datenbank ausführen.

Ein Profil kann nur auf eine Datenbank verweisen. Auf dieselbe Datenbank kann mit mehr als einem Profil verwiesen werden. Auf Backups, die mit einem Profil erstellt werden, kann nicht über ein anderes Profil zugegriffen werden, auch wenn beide Profile auf dieselbe Datenbank verweisen.

Profilinformationen werden in einem Repository gespeichert. Das Repository enthält sowohl die Profilinformationen für die Datenbank als auch Informationen zu den Snapshot-Kopien, die als Datenbank-Backup dienen. Die tatsächlichen Snapshot Kopien werden im Storage-System gespeichert. Die Namen der Snapshot Kopie werden im Repository gespeichert, das das Profil für diese Datenbank enthält. Wenn Sie einen Vorgang in einer Datenbank ausführen, müssen Sie das Profil aus dem Repository auswählen.

Die folgende Abbildung zeigt, wie Repositories mehrere Profile aufnehmen können, aber auch dass jedes Profil nur eine Datenbank definieren kann:



Im vorhergehenden Beispiel befindet sich Repository2 auf Datenbank DB1 und Repository1 befindet sich auf der Datenbank DB4.

Jedes Profil enthält die Anmeldeinformationen für die Datenbank, die mit dem Profil verknüpft ist. Mit den Anmeldeinformationen kann SnapManager eine Verbindung zur Datenbank herstellen und mit der Datenbank arbeiten. Die gespeicherten Anmeldeinformationen umfassen den Benutzernamen und die Kennwortpaare für den Zugriff auf den Host, das Repository, die Datenbank und die erforderlichen Verbindungsinformationen, wenn Sie Oracle Recovery Manager (RMAN) verwenden.

Sie können nicht auf ein Backup zugreifen, das mit einem Profil aus einem anderen Profil erstellt wurde, auch wenn beide Profile mit derselben Datenbank verknüpft sind. SnapManager legt eine Sperre auf die Datenbank ab, um zu verhindern, dass zwei inkompatible Vorgänge gleichzeitig ausgeführt werden.

Profil zur Erstellung vollständiger und partieller Backups

Sie können Profile erstellen, um vollständige Backups oder partielle Backups zu erstellen.

Die Profile, die Sie zur Erstellung der vollständigen und partiellen Backups angeben, enthalten sowohl die Datendateien als auch die Archivprotokolldateien. SnapManager erlaubt solche Profile nicht, die Backups des Archivprotokolls von den Backups der Datendatei zu trennen. Die vollständigen und teilweisen Backups werden basierend auf den vorhandenen Richtlinien zur Backup-Aufbewahrung aufbewahrt und basierend auf den vorhandenen Sicherungsrichtlinien geschützt. Sie können vollständige und teilweise Backups basierend auf der zu Ihnen passt Uhrzeit und Häufigkeit planen.

Profile für die Erstellung von datenbasierten Backups und nur-Archiv-Backups

Mit SnapManager (3.2 oder höher) können Sie Profile erstellen, die Backups der Archivprotokolldateien getrennt von den Datendateien machen. Nachdem Sie das Profil zur Trennung der Backup-Typen verwendet haben, können Sie entweder Datendateien-only-Backups oder lediglich Archiv-Log-Backups der Datenbank erstellen. Sie können auch ein Backup erstellen, das sowohl die Datendateien als auch die Archivprotokolldateien enthält.

Die Aufbewahrungsrichtlinie gilt für alle Datenbank-Backups, wenn die Archiv-Log-Backups nicht getrennt sind. Nachdem Sie die Backups für das Archivprotokoll getrennt haben, können Sie in SnapManager unterschiedliche Aufbewahrungszeiträume und Sicherungsrichtlinien für die Backups des Archivierungsprotokolls festlegen.

Aufbewahrungsrichtlinie

SnapManager legt fest, ob ein Backup aufbewahrt werden soll, indem sowohl die Anzahl der Aufbewahrung (z. B. 15 Backups) als auch die Aufbewahrungsdauer (z. B. 10 Tage tägliche Backups) berücksichtigt werden. Ein Backup läuft ab, wenn sein Alter die für seine Aufbewahrungsklasse festgelegte Aufbewahrungsdauer überschreitet und die Anzahl der Backups die Anzahl der Backups übersteigt. Beispiel: Wenn die Backup-Anzahl 15 beträgt (was bedeutet, dass SnapManager 15 erfolgreiche Backups erstellt hat) und die Dauer für tägliche Backups von 10 Tagen festgelegt wurde, verfallen die fünf ältesten, erfolgreichen und infrage kommenden Backups.

Aufbewahrungsdauer des Archivprotokolls

Nach Trennung der Backup-Protokolle werden sie basierend auf der Aufbewahrungsdauer des Archivprotokolls aufbewahrt. Backups von Archivprotokolldateien, die mit Backups von Datendateien erstellt werden, werden immer zusammen mit Backups dieser Datendateien aufbewahrt, unabhängig von der Aufbewahrungsdauer für das Archivprotokoll.

Verwandte Informationen

Profilverwaltung für effiziente Backups

Die Status der SnapManager-Operation lauten

SnapManager-Vorgänge (Backup, Wiederherstellung und Klon) können den jeweiligen Status aufweisen, wobei jeder Status den Fortschritt des Vorgangs angibt.

Betriebsstatus	Beschreibung
Erfolgreich	Die Operation wurde erfolgreich abgeschlossen.

Betriebsstatus	Beschreibung
Wird Ausgeführt	Der Vorgang wurde gestartet, ist aber noch nicht abgeschlossen. Ein Backup, das zwei Minuten dauert, wird beispielsweise um 11:00 Uhr morgens erstellt. Wenn Sie die Registerkarte **Zeitplan** um 11:01 Uhr aufrufen, wird der Vorgang als ausgeführt angezeigt.
Kein Vorgang gefunden	Der Zeitplan wurde nicht ausgeführt oder das letzte Backup wurde gelöscht.
Fehlgeschlagen	Der Vorgang ist fehlgeschlagen. SnapManager hat den Abbruchvorgang automatisch ausgeführt und den Vorgang bereinigt. **Hinweis:** Sie können den erstellten Klon teilen. Wenn Sie den geteilten Klon-Vorgang beenden, den Sie gestartet haben und der Vorgang erfolgreich angehalten wurde, wird der Status des Klon-Split-Vorgangs als fehlgeschlagen angezeigt.

Wiederherstellbare und nicht wiederherstellbare Ereignisse

Ein wiederherstellbares SnapManager Ereignis hat die folgenden Probleme:

- Die Datenbank wird nicht auf einem Storage-System gespeichert, auf dem Data ONTAP ausgeführt wird.
- Eine ASM-Datenbank (Automatic Storage Management) wird konfiguriert, die ASM-Instanz wird jedoch nicht ausgeführt.
- SnapDrive für UNIX ist nicht installiert oder kann nicht auf das Speichersystem zugreifen.
- SnapManager erstellt keine Snapshot Kopie bzw. stellt keinen Storage bereit, wenn das Volume über keinen freien Speicherplatz verfügt, die maximale Anzahl an Snapshot Kopien erreicht oder eine unerwartete Ausnahme auftritt.

Wenn ein wiederherstellbares Ereignis eintritt, wird SnapManager abgebrochen und versucht, den Host, die Datenbank und das Storage-System auf den Startstatus zurückzusetzen. Schlägt der Abbruchvorgang fehl, behandelt SnapManager den Vorfall als nicht wiederherstellbares Ereignis.

Wenn eines der folgenden Ereignisse eintritt, tritt ein nicht behebbares (Out-of-Band)-Ereignis auf:

- Ein Systemproblem tritt auf, z. B. wenn ein Host ausfällt.
- Der SnapManager-Prozess wird angehalten.
- Der Abbruch innerhalb des Band schlägt fehl, wenn das Speichersystem ausfällt, die Nummer der logischen Einheit (LUN) oder das Speichervolume offline ist oder das Netzwerk ausfällt.

Wenn ein nicht behebbares Ereignis eintritt, wird SnapManager sofort abgebrochen. Der Host, die Datenbank und das Speichersystem sind möglicherweise nicht an den ursprünglichen Status zurückgekehrt. In diesem Fall müssen Sie nach Ausfall des SnapManager-Vorgangs eine Bereinigung durchführen, indem Sie die verwaiste Snapshot Kopie löschen und die SnapManager-Sperrdatei entfernen.

Wenn Sie die SnapManager-Sperrdatei löschen möchten, navigieren Sie auf dem Zielcomputer zu Oracle_HOME €und löschen Sie die Datei SM_Lock_TargetDBName. Nach dem Löschen der Datei müssen Sie den SnapManager für Oracle-Server neu starten.

Wie SnapManager die Sicherheit gewährleistet

Sie können SnapManager Vorgänge nur ausführen, wenn Sie die entsprechenden Anmeldedaten besitzen. Die Sicherheit in SnapManager unterliegt der Benutzerauthentifizierung und der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC). RBAC ermöglicht Datenbankadministratoren die Einschränkung von Vorgängen, die SnapManager auf den Volumes und LUNs ausführen kann, die die Datendateien in einer Datenbank enthalten.

Datenbankadministratoren ermöglichen die rollenbasierte Zugriffssteuerung für SnapManager mithilfe von SnapDrive. Datenbankadministratoren weisen anschließend SnapManager-Rollen Berechtigungen zu und weisen diese Rollen den Benutzern in der grafischen Benutzeroberfläche (GUI) oder der Befehlszeilenschnittstelle (CLI) von Operations Manager zu. RBAC-Berechtigungsprüfungen erfolgen im DataFabric Manager Server.

Zusätzlich zum rollenbasierten Zugriff behält SnapManager die Sicherheit bei, indem er die Benutzerauthentifizierung über Passwortaufforderungen oder die Festlegung von Benutzeranmeldeinformationen anfordert. Ein effektiver Benutzer wird beim SnapManager-Server authentifiziert und autorisiert.

Die SnapManager Anmeldedaten und die Benutzerauthentifizierung unterscheiden sich erheblich von SnapManager 3.0:

- In SnapManager-Versionen vor 3.0 würden Sie bei der Installation von SnapManager ein willkürliches Serverkennwort festlegen. Wer den SnapManager-Server nutzen möchte, braucht das SnapManager-Server-Passwort. Das SnapManager-Server-Passwort muss den Benutzeranmeldeinformationen mit dem smo-Befehl „set-serm“ hinzugefügt werden.
- In SnapManager (3.0 und höher) wurde das SnapManager-Serverpasswort durch die Authentifizierung des individuellen Betriebssystems (OS) ersetzt. Wenn Sie den Client nicht vom selben Server wie den Host ausführen, führt der SnapManager-Server die Authentifizierung durch, indem Sie die Benutzernamen und Passwörter des Betriebssystems verwenden. Wenn Sie nicht zur Eingabe Ihrer OS-Passwörter aufgefordert werden möchten, können Sie die Daten unter Verwendung des Befehls smo cridential set -Host im SnapManager-Benutzeranmeldungs-Cache speichern.

> Der Befehl smo Anmeldeinformation set -Host speichert Ihre Anmeldeinformationen, wenn die Eigenschaft Host.anmeldungs.persist in der Datei smo.config auf true gesetzt ist.

Beispiel

Benutzer1 und User2 teilen sich ein Profil namens Prof2. User2 kann eine Sicherung von „database1“ in Host1 nicht ohne die Berechtigung zum Zugriff auf Host1 durchführen. User1 kann eine Datenbank nicht ohne Berechtigung zum Zugriff auf host3 klonen.

In der folgenden Tabelle werden die verschiedenen Berechtigungen beschrieben, die den Benutzern zugewiesen sind:

Berechtigungstyp	Benutzer1	Benutzer2
Host-Passwort	Host1, Host2	Host2, Host3
Repository-Kennwort	Repos. 1	Repos. 1

Profilkennwort	Prof1, Prof2	Prof2

Wenn User1 und User2 keine freigegebenen Profile haben, nimmt an, dass User1 Berechtigungen für die Hosts mit Namen Host1 und Host2 hat, und User2 hat Berechtigungen für den Host namens Host2. User2 kann nicht einmal die nicht-profilbefehlen wie dump und System verify auf Host1 ausführen.

Online-Hilfe aufrufen und drucken

Die Online-Hilfe enthält Anweisungen zu den Aufgaben, die Sie über die grafische Benutzeroberfläche von SnapManager ausführen können. Die Online-Hilfe enthält auch Beschreibungen der Felder in den Fenstern und Assistenten.

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Hauptfenster auf **Hilfe** > **Hilfe Inhalt**.
   - Klicken Sie in einem beliebigen Fenster oder Assistenten auf **Hilfe**, um Hilfe für dieses Fenster anzuzeigen.
2. Verwenden Sie das **Inhaltsverzeichnis** im linken Fensterbereich, um durch die Themen zu navigieren.
3. Klicken Sie oben im Hilfefenster auf das Druckersymbol, um einzelne Themen zu drucken.

Empfohlene allgemeine Datenbanklayouts und Speicherkonfigurationen

Durch das Wissen der empfohlenen allgemeinen Datenbank-Layouts und Storage-Konfigurationen können Sie Probleme in Bezug auf Festplattengruppen, Dateitypen und Tablespaces vermeiden.

- Fügen Sie keine Dateien aus mehr als einem SAN-Dateisystem oder Volume-Manager in Ihre Datenbank ein.

  Alle Dateien, die eine Datenbank erstellen, müssen sich auf demselben Dateisystem befinden.

- SnapManager erfordert mehrere 4 KB Blockgröße.
- Fügen Sie die Datenbank-System-ID in die oratab-Datei ein.

  Fügen Sie für jede zu verwaltende Datenbank einen Eintrag in die Oratab-Datei ein. SnapManager verlässt sich darauf, dass die oratab-Datei das Zuhause von Oracle bestimmt.

- Wenn Sie SnapManager-Backups mit dem Oracle Recovery Manager (RMAN) registrieren möchten, müssen Sie RMAN-fähige Profile erstellen.

Wenn Sie die neue Volume-basierte Wiederherstellung oder vollständige Laufwerksgruppenswiederherstellung nutzen möchten, sollten Sie die folgenden Richtlinien in Bezug auf Dateisysteme und Laufwerksgruppen berücksichtigen:

- Mehrere Datenbanken können nicht dieselbe ASM-Laufwerksgruppe (Automatic Storage Management) verwenden.
- Eine Laufwerksgruppe, die Datendateien enthält, kann keine anderen Dateitypen enthalten.
- Die LUN (Logical Unit Number) für die Datendatei-Festplattengruppe muss das einzige Objekt im Storage-Volume sein.

Nachfolgend sind einige Richtlinien für die Volume-Trennung aufgeführt:

- Die Datendateien für nur eine Datenbank müssen sich im Volume befinden.
- Sie müssen separate Volumes für jede der folgenden Dateiklassifizierungen verwenden: Datenbankbinärdateien, Datendateien, Online-Wiederherstellungsprotokolle, archivierte Wiederherstellungsprotokolle und Kontrolldateien.
- Sie müssen kein separates Volume für temporäre Datenbankdateien erstellen, da SnapManager keine temporären Datenbankdateien erstellt.

Definieren des Datenbank-Home mit der oratab-Datei

SnapManager verwendet die oratab-Datei während Operationen, um das Home-Verzeichnis der Oracle-Datenbank zu bestimmen. Ein Eintrag für Ihre Oracle-Datenbank muss in der oratab-Datei sein, damit SnapManager ordnungsgemäß funktionieren kann. Die oratab-Datei wird während der Oracle-Softwareinstallation erstellt.

Die oratab-Datei befindet sich an verschiedenen Orten, basierend auf dem Host-Betriebssystem, wie in der folgenden Tabelle dargestellt:

Host-Betriebssystem	Speicherort der Datei
Linux	/Etc/oratab
Solaris	/Var/opt/oracle/oratab
IBM AIX	/Etc/oratab

Die Beispiel-Oratab-Datei enthält die folgenden Informationen:

```
+ASM1:/u01/app/11.2.0/grid:N   # line added by Agent
oelpro:/u01/app/11.2.0/oracle:N         # line added by Agent
# SnapManager generated entry          (DO NOT REMOVE THIS LINE)
smoclone:/u01/app/11.2.0/oracle:N
```

Nach der Installation von Oracle müssen Sie sicherstellen, dass sich die oratab-Datei in dem in der vorherigen Tabelle angegebenen Speicherort befindet. Wenn sich die oratab-Datei nicht an dem richtigen Ort gemäß Ihrem Betriebssystem befindet, müssen Sie sich an den technischen Support wenden, um Hilfe zu erhalten.

Anforderungen für die Verwendung von RAC-Datenbanken mit SnapManager

Sie müssen die Empfehlungen für die Verwendung von RAC-Datenbanken (Real Application Clusters) mit SnapManager kennen. Die Empfehlungen umfassen Portnummern, Passwörter und den Authentifizierungsmodus.

- Im Datenbankauthentifizierungsmodus muss der Listener auf jedem Knoten, der mit einer Instanz der RAC-Datenbank interagiert, so konfiguriert werden, dass er dieselbe Portnummer verwendet.

Der Listener, der mit der primären Datenbankinstanz interagiert, muss vor dem Start eines Backups gestartet werden.

- Im Betriebssystem-Authentifizierungsmodus oder in einer ASM-Umgebung (Automatic Storage Management) muss der SnapManager-Server auf jedem Knoten der RAC-Umgebung installiert und ausgeführt werden.
- Das Benutzerpasswort für die Datenbank (z. B. für einen Systemadministrator oder einen Benutzer mit der sysdba-Berechtigung) muss für alle Oracle-Datenbankinstanzen in einer RAC-Umgebung identisch sein.

Anforderungen für die Verwendung von ASM-Datenbanken mit SnapManager

Sie müssen die Anforderungen für die Verwendung von ASM-Datenbanken (Automatic Storage Management) mit SnapManager kennen. Wenn Sie diese Anforderungen kennen, können Sie unter anderem Probleme mit den Spezifikationen ASMLib, Partitionen und Klonen vermeiden.

- SnapManager (3.0.3 oder höher) verwendet die neue sysasm-Berechtigung, die mit Oracle 11gR2 verfügbar ist, anstatt die sysdba-Berechtigung zur Verwaltung einer Oracle ASM-Instanz.

  Wenn Sie die sysdba-Berechtigung zum Ausführen von Administratorbefehlen auf der ASM-Instanz verwenden, wird eine Fehlermeldung angezeigt. Die Datenbank verwendet die sysdba-Berechtigung für den Zugriff auf Laufwerksgruppen. Wenn Sie eine Verbindung mit der ASM-Instanz über die sysasm-Berechtigung herstellen, haben Sie vollständigen Zugriff auf alle verfügbaren Oracle ASM-Festplattengruppen und Verwaltungsfunktionen.

  Wenn Sie Oracle 10gR2 und 11gR1 verwenden, müssen sie weiterhin die sysdba-Berechtigung verwenden.

- SnapManager (3.0.3 oder höher) unterstützt die Sicherung von Datenbanken, die direkt auf ASM-Festplattengruppen gespeichert sind, wenn die Laufwerksgruppe auch ein ACFS-Volume (Automatic Cluster File System) enthält.

  Diese Dateien sind indirekt durch SnapManager geschützt und werden möglicherweise mit dem restlichen Inhalt einer ASM-Festplattengruppe wiederhergestellt, aber SnapManager (3.0.3 oder höher) unterstützt kein ACFS.

  ACFS ist eine plattformübergreifende, skalierbare File-System-Storage-Management-Technologie, die mit Oracle 11gR2 verfügbar ist. ACFS erweitert die ASM-Funktionalität, um Kundendateien zu unterstützen, die außerhalb der Oracle-Datenbank gepflegt werden.

- SnapManager (3.0.3 oder höher) unterstützt die Sicherung von Dateien, die auf ASM-Festplattengruppen gespeichert sind, wenn die Laufwerksgruppe auch OCR-Dateien (Oracle Cluster Registry) oder Abstimmdiskdateien enthält. Wiederherstellungsvorgänge erfordern jedoch eine langsamere, hostbasierte oder PFSR-Methode (Partial File Snap Restore).

  Am besten sollten OCR- und Abstimmfestplatten auf Laufwerksgruppen vorhanden sein, die keine Datenbankdateien enthalten.

- Jedes für ASM verwendete Laufwerk darf nur eine Partition enthalten.
- Die Partition, die die ASM-Daten hostet, muss richtig ausgerichtet sein, um schwere Performanceprobleme zu vermeiden.

Dies bedeutet, dass die LUN den korrekten Typ haben muss, und die Partition einen Offset mit einem mehrere 4K Byte haben muss.

Weitere Informationen zum Erstellen von Partitionen, die auf 4K ausgerichtet sind, finden Sie im Knowledge Base-Artikel 1010717.

- ASM-Konfiguration ist nicht als Teil der Klonspezifikation angegeben.

  Sie müssen die ASM-Konfigurationsinformationen in den Klonspezifikationen, die mit SnapManager 2.1 erstellt wurden, manuell entfernen, bevor Sie den Host auf SnapManager (2.2 oder höher) aktualisieren.

- SnapManager 3.1, 3.1p1 und 3.2 oder höher unterstützen ASMLib 2.1.4.
- SnapManager 3.1p4 oder höher unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8.

Unterstützte Partitionsgeräte

Sie müssen die verschiedenen Partitionsgeräte kennen, die in SnapManager unterstützt werden.

Die folgende Tabelle enthält Partitionsinformationen und die Möglichkeit, diese für verschiedene Betriebssysteme zu aktivieren:

Betriebssystem	Einzelne Partition	Mehrere Partitionen	Geräte ohne Partitionierung	Dateisystem oder RAW-Geräte
Red hat Enterprise Linux 5x oder Oracle Enterprise Linux 5-mal	Ja.	Nein	Nein	Ext3*
Red hat Enterprise Linux 6 x oder Oracle Enterprise Linux 6x	Ja.	Nein	Nein	Ext3 oder ext4*
SUSE Linux Enterprise Server 11	Ja.	Nein	Nein	Ext3*
SUSE Linux Enterprise Server 10	Nein	Nein	Ja.	Erw. 3***
Red hat Enterprise Linux 5x oder Lateror Oracle Enterprise Linux 5-mal oder höher	Ja.	Nein	Ja.	ASM mit ASMlib**

Betriebssystem	Einzelne Partition	Mehrere Partitionen	Geräte ohne Partitionierung	Dateisystem oder RAW-Geräte
SUSE Linux Enterprise Server 10 SP4or SUSE Linux Enterprise Server 11	Ja.	Nein	Ja.	ASM mit ASMlib**
SUSE Linux Enterprise Server 10 SP4 oder Lateror SUSE Linux Enterprise Server 11	Ja.	Nein	Nein	ASM ohne ASMlib**

Weitere Informationen zu den unterstützten Betriebssystemversionen finden Sie in der Interoperabilitäts-Matrix.

Unterstützung für ASMLib

SnapManager unterstützt verschiedene Versionen von ASMLib, obwohl es mehrere Faktoren, die Sie bei der Verwendung von SnapManager mit ASMLib berücksichtigen müssen.

SnapManager unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8. Alle SnapManager-Vorgänge können mit ASMLib 2.1.4, 2.1.7 und 2.1.8 ausgeführt werden.

Wenn Sie von ASMLib 2.1.4 auf ASM 2.1.7 aktualisiert haben, können Sie die gleichen Profile und Backups verwenden, die mit ASMLib 2.1.4 erstellt wurden, um die Backups wiederherzustellen und die Klone zu erstellen.

Bei der Verwendung von SnapManager mit ASMLib müssen Sie Folgendes berücksichtigen:

- SnapManager 3.1 unterstützt ASMLib 2.1.7 nicht.

  SnapManager 3.1p4 oder höher unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8.

- Nach einem Rolling Upgrade von SnapManager 3.1 auf 3.2 funktionieren die mit ASMLib 2.1.7 erstellten Backups nur dann, wenn das Repository wieder auf SnapManager 3.1 und ASMLib 2.1.7 zurückgesetzt wird auf ASMLib 2.1.4.
- Nach einem Rolling Upgrade von SnapManager 3.1 auf 3.2 funktionieren Backups, die mit ASMLib 2.1.7 7 erstellt wurden, nicht, wenn das Repository mit ASMLib 2.1 zurück zu SnapManager 3.1 zurückgesetzt wird.

  Das Rollback ist erfolgreich, aber die Profile und Backups können nicht verwendet werden.

Unterstützung für ASM-Datenbanken ohne ASMLib

SnapManager unterstützt standardmäßig ASM ohne ASMLib. Die grundlegende Voraussetzung ist, dass die Geräte, die für ASM-Laufwerksgruppen verwendet werden,

partitioniert werden müssen.

Wenn ASMLib nicht installiert ist, werden die Geräteberechtigungen für ASM-Laufwerksgruppen in root:Disk geändert, wenn Sie die folgenden Vorgänge ausführen:

- Starten Sie den Host neu
- Wiederherstellen einer Datenbank aus dem primären Storage mithilfe von Volume-basierten SnapRestore (VBSR)
- Wiederherstellung einer Datenbank aus dem sekundären Storage

Sie können die entsprechenden Geräteberechtigungen festlegen, indem Sie der Konfigurationsoption oracleasm.Support.without.asmlib in smo.conf True zuweisen. Die mit den ASM-Laufwerksgruppen verbundenen Geräte werden beim Hinzufügen oder Entfernen neuer Geräte vom Host hinzugefügt oder aus der Datei initasmdisk entfernt. Die Datei initasmdics befindet sich unter /etc/initasmDisks.

Wenn Sie beispielsweise oracleasm.Support.without.asmlib=true festlegen und anschließend eine Sicherungshalterung durchführen, werden neue Geräte zu initasmDisks hinzugefügt. Beim Neustart des Hosts werden die Geräteberechtigungen und die Eigentumsrechte von den Startskripten beibehalten.

Der Standardwert für oracleasm.Support.without.asmlib ist false.

Verwandte Informationen

Unterstützte Partitionsgeräte

Unterstützte Skripte

Die Skripte asmmain.sh und asmquerydisk.sh ermöglichen das Ändern des Grid-Benutzers, der Gruppe und des Benutzers, die alle zur Abfrage der ASM-Laufwerke verwendet werden. Die Skripte müssen immer aus dem Root ausgeführt werden.

Die asmmain.sh ist die Skript-Hauptdatei, die von jedem Vorgang aufgerufen wird, der Geräte hinzufügt oder löscht. Das Skript asmmain.sh ruft intern ein anderes Skript auf, das vom Root ausgeführt werden muss, das über oracle Grid-Anmeldedaten verfügt. Dieses Skript fragt die Geräte der ASM-Laufwerksgruppe ab und fügt diese Einträge in der initasmdisk-Datei mit der Berechtigung und dem Eigentum der Geräte hinzu. Sie können die Berechtigungen und Eigentumsrechte dieser Datei basierend auf Ihrer Umgebung und dem regex-Muster ändern, das nur zur Übereinstimmung mit /dev/mapper/*p1 verwendet wird.

Das Skript asmquerydisk.sh wird verwendet, um die Festplattenliste abzufragen, die zur Erstellung der ASM-Laufwerksgruppe verwendet wird. Je nach Konfiguration müssen Sie Oracle_BASE, ORACLE_HOME und ORACLE_SID Werte zuweisen.

Die Skripte finden sich unter /opt/NetApp/smo/Plugins/examples/noasmlib. Diese Skripte müssen allerdings in die /opt/NetApp/smo/Plugins/noasmlib verschoben werden, bevor der SnapManager für Oracle Server auf dem Host gestartet wird.

Einschränkungen bei der Verwendung von Skripten zur Unterstützung einer ASM-Datenbank ohne ASMLib

Sie müssen sich über bestimmte Einschränkungen bei der Verwendung von Skripten zur Unterstützung einer ASM-Datenbank ohne ASMLib bewusst sein.

- Die Skripte stellen eine alternative Lösung für jede Kernel-Version dar, jedoch nur, wenn ASMLib nicht installiert ist.

- Die Berechtigungen für die Skripte müssen so festgelegt werden, dass Root-, Grid-, oracle- oder vergleichbare Benutzer auf die Skripte zugreifen können.
- Die Skripte unterstützen keine Wiederherstellung von einem sekundären Speicherort.

Implementieren und Ausführen der Skripte

Sie können die Skripte asmmain.sh und asmquerydisk.sh bereitstellen und ausführen, um ASM-Datenbanken ohne ASMLib zu unterstützen.

Diese Skripte folgen nicht der Pre-scripts oder Post-scripts Syntax und Workflow wird aufgerufen, wenn intitasmdisks aktiviert ist. Sie können in den Skripten alles ändern, was mit Ihren Konfigurationseinstellungen zusammenhängt. Es wird empfohlen zu überprüfen, ob alle Skripte mit einem kurzen Trockenlauf wie erwartet funktionieren.

> Diese Skripte schaden Ihrem System weder bei Ausfällen noch werden sie Ihr System beeinträchtigen. Diese Skripte werden ausgeführt, um die ASM-bezogenen Laufwerke zu aktualisieren, um die richtigen Berechtigungen und Eigentumsrechte zu haben, so dass die Festplatten immer unter ASM-Instanz Kontrolle.

1. Erstellen Sie die ASM-Festplattengruppen mit den partitionierten Laufwerken.
2. Erstellen Sie die Oracle-Datenbank auf den FESTPLATTENGRUPPEN.
3. Beenden Sie den SnapManager für Oracle Server.

   > In einer RAC-Umgebung müssen Sie diesen Schritt auf allen RAC-Knoten durchführen.

4. Ändern Sie die smo.conf, um die folgenden Parameter einzuschließen:

   a. Oracleasm.Support.without.asmlib = true
   b. Oracleasm.Support.without.asmlib.Ownership = true
   c. oracleasm.support.without.asmlib.username = Benutzername Ihrer ASM-Instanzumgebung
   d. oracleasm.support.without.asmlib.groupname = Gruppenname Ihrer ASM-Instanzumgebung

   Durch diese Änderungen werden nur die Berechtigungen für den absoluten Pfad festgelegt, was bedeutet, dass anstelle des Partitionsgeräts die Berechtigungen nur für das dm-*-Gerät festgelegt werden.

5. Fügen Sie die Konfigurationseinstellungen in die Skripte der Plug-ins unter /opt/NetApp/smo/examples/noasmlib ein.
6. Kopieren Sie die Skripte in /opt/NetApp/smo/Plugins/noasmlib, bevor Sie den SnapManager für Oracle Server auf dem Host starten.
7. Navigieren Sie zum Verzeichnis /opt/NetApp/smo und führen Sie einen trockenen Lauf durch: sh Plug-ins/noasmlib/asmmain.sh

   Die etc/initasmdisks-Datei wird erstellt, was die Hauptdatei ist, die verwendet wird.

   Sie können bestätigen, dass die etc/initasmdisks-Datei alle Geräte enthält, die mit der konfigurierten ASM-Datenbank zusammenhängen, wie z. B.:

```
chown -R grid:oinstall /dev/mapper/360a98000316b61396c3f394645776863p1
         chmod 777 /dev/mapper/360a98000316b61396c3f394645776863p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714239p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714239p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714241p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714241p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714243p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714243p1
```

8. Starten Sie den SnapManager für Oracle-Server.
9. Konfigurieren Sie SnapDrive für UNIX, indem Sie die folgende Datei zur snapdrive.conf Datei hinzufügen.Disconnect-luns-before-vbsr=on
10. Starten Sie SnapDrive für UNIX Server neu.

> In einer RAC-Umgebung müssen Sie die Schritte 3 bis 10 für alle RAC-Knoten durchführen.

Die erstellte /etc/initasmdics-Datei muss entweder aus einem der Startskripte oder aus einem Skript ausgeführt werden, das in rc3.d. neu definiert ist Die Datei /etc/initasmdisks sollte immer ausgeführt werden, bevor der oracleha-Dienst gestartet wird.

Beispiel

```
# ls -ltr *ohasd*
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 S96ohasd ->
/etc/init.d/ohasd
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 K15ohasd ->
/etc/init.d/ohasd
```

Im folgenden Beispiel ist sh -x/etc/initasmdisks standardmäßig nicht verfügbar, und Sie müssen es als die erste Zeile der Funktion anhängen `start_stack()` In einem ohasd-Skript:

```
start_stack()
{
sh -x /etc/initasmdisks
# see init.ohasd.sbs for a full rationale case $PLATFORM in Linux
}
```

Unterstützung für Oracle RAC ASM-Datenbanken ohne ASMLib

Wenn Sie Oracle RAC-Datenbanken verwenden, müssen die RAC-Knoten mit der

Initasmdics-Datei aktualisiert werden, sobald ein Vorgang im Master RAC-Knoten ausgeführt wird.

Wenn sich vom Master-Knoten aus keine Authentifizierung bei den RAC-Knoten anmelden muss, führt der asmmain.sh eine sichere Kopie (SCP) von InitasmDisks an alle RAC-Knoten aus. Die InitasmDisks-Datei des Master-Knotens wird jedes Mal aufgerufen, wenn eine Wiederherstellung stattfindet. Das Skript asmmain.sh kann aktualisiert werden, um auf alle RAC-Knoten dasselbe Skript aufzurufen.

Die erstellte /etc/initasmdics-Datei, die entweder aus einem der Startskripte oder aus einem neu definierten Skript in rc3.d. ausgeführt werden muss Die Datei /etc/initasmdisks sollte immer ausgeführt werden, bevor der oracleha-Dienst gestartet wird.

Unterstützung für Oracle 10g ASM-Datenbanken ohne ASMLib

Wenn Sie Oracle 10g verwenden, steht der Befehl asmcmd nicht für die Auflistung von Disketten zur Verfügung. Sie können die sql-Abfrage verwenden, um die Festplattenliste abzurufen.

Das Script Disk_list.sql ist in die vorhandenen Skripte enthalten, die im Beispielverzeichnis zur Unterstützung von sql-Abfragen zur Verfügung gestellt werden. Wenn Sie theasmquerydisk.sh Skript ausführen, muss das Script Disk_list.sql manuell ausgeführt werden. Die Beispielzeilen werden mit Kommentaren in der Datei asmquerydisk.sh hinzugefügt. Diese Datei kann entweder am Speicherort /Home/Grid oder an einem anderen Ort Ihrer Wahl platziert werden.

Beispielskripts zur Unterstützung von ASM-Datenbanken ohne ASMLib

Die Beispielskripte sind im Verzeichnis Plugins/examples/noasmlib des Installationsverzeichnisses für SnapManager für Oracle verfügbar.

asmmain.sh

```
#!/bin/bash
griduser=grid
gridgroup=oinstall

# Run the script which takes the disklist from the asmcmd
# use appropriate user , here grid user is being used to run
# asmcmd command.
su -c "plugins/noasmlib/asmdiskquery.sh" -s /bin/sh grid
cat /home/grid/disklist

# Construct the final file as .bak file with propre inputs
awk -v guser=$griduser -v ggroup=$gridgroup '/^\/dev\/mapper/ { print
"chown -R "guser":"ggroup" "$1; print "chmod 777 " $1; }'
/home/grid/disklist > /etc/initasmdisks.bak

# move the bak file to the actual file.
mv /etc/initasmdisks.bak /etc/initasmdisks
```

```
# Set full full permission for this file to be called while rebooting and
restore
chmod 777 /etc/initasmdisks

# If the /etc/initasmdisks needs to be updated in all the RAC nodes
# or /etc/initasmdisks script has to be executed in the RAC nodes, then
the following
# section needs to be uncommented and used.
#
# Note: To do scp or running scripts in remote RAC node via ssh, it needs
password less login
# for root user with ssh keys shared between the two nodes.
#
# The following 2 lines are used for updating the file in the RAC nodes:
# scp /etc/initasmdisks root@racnode1:/etc/initasmdisks
# scp /etc/initasmdisks root@racnode2:/etc/initasmdisks
#
# In order to execute the /etc/initasmdisks in other RAC nodes
# The following must be added to the master RAC node /etc/initasmdisks
file
# from the asmmain.sh script itself. The above scp transfer will make sure
# the permissions and mode for the disk list contents are transferred to
the other RAC nodes
# so now appending any command in the /etc/initasmsdisks will be retained
only in the master RAC node.
# The following lines will add entries to the /etc/initasmsdisks file in
master RAC node only. When this script is executed
#  master RAC node, /etc/initasmdisks in all the RAC nodes will be
executed.
# echo 'ssh racnode1 /etc/initasmdisks' >> /etc/initasmdisks
# echo 'ssh racnode2 /etc/initasmdisks' >> /etc/initasmdisks
```

asmquerydisk.sh

```
#!/bin/bash
export  ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/grid/product/11.2.0.3/grid
export ORACLE_SID=+ASM
export  PATH=$ORACLE_HOME/bin:$PATH

# Get the Disk List and save this in a file called dglist.
asmcmd lsdsk  > /home/grid/disklist

# In oracle 10g the above used command 'asmcmd' is not available so use
SQL
# query can be used to take the disk list. Need to uncomment the following
# line and comment the above incase oracle 10g is being in use.
# The disk_list.sql script is availbe in this noasmlib examples folder
itself
# which can be modified as per customer needs.
# sqlplus "/as sysdba" @/home/grid/disk_list.sql > /home/grid/disklist
```

Disk_list.sql

```
# su - oracle
-bash-4.1$ cat disk_list.sql
select path from v$asm_disk;
exit
-bash-4.1$
```

Anforderungen für die Verwendung von Datenbanken mit NFS und SnapManager

Sie müssen die Anforderungen für die Verwendung von Datenbanken mit Network File System (NFS) und SnapManager kennen. Die Empfehlungen umfassen die Ausführung als root, Attribut-Caching und symbolische Links.

- Sie müssen SnapManager als Root ausführen. SnapManager muss auf die Dateisysteme zugreifen können, die Datendateien, Kontrolldateien, Online-Wiederherstellungsprotokolle, Archivprotokolle und den Datenbank-Home enthalten.

  Legen Sie eine der folgenden NFS-Exportoptionen fest, um sicherzustellen, dass Root auf die Dateisysteme zugreifen kann:

  - Root=Hostname
  - rw=Host-Name, anon=0
- Sie müssen das Attribut-Caching für alle Volumes deaktivieren, die Datenbankdatendateien, Kontrolldateien, Redo- und Archivprotokolle und die Datenbank-Startseite enthalten.

  Exportieren Sie die Volumes mithilfe der optionen noac (für Solaris und AIX) oder actimeo=0 (für Linux).

- Sie müssen die Datenbankdatendateien aus dem lokalen Speicher mit NFS verknüpfen, um nur symbolische Links auf Mount-Punkt-Ebene zu unterstützen.

Beispiel für Datenbank-Volume-Layouts

Weitere Informationen zur Konfiguration Ihrer Datenbank finden Sie unter Beispiel-Datenbank-Volume-Layouts.

Single-Instance-Datenbanken

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_sid	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_sid (Multiplexed) Oralogen02_sid (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Ja.	Aus

RAC-Datenbanken (Real Application Clusters)

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_dbname	Ja.	Aus
Temporäre Datendateien	Oratepp_dbname	Ja.	Aus
Kontrolldateien	Oracntrl01_dbname (Multiplexed) Oracntrl02_dbname (Multiplexed)	Ja.	Aus

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_dbname	Ja.	Aus
Cluster-Dateien	Oracrs_clustername	Ja.	Ein

Einzelne Instanz einer ASM-Datenbank (Automatic Storage Management

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Orabin_Host namelun	Ja.	Ein
Datendateien	Oradata_sid	Oradata_sidlun	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Oratepp_sidlun	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Oracntrl01_sidlun (Multiplexed) Oracntrl02_sidlun (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Oralog01_dbnamelun (Multiplexed) Oralogen02_dbnamelun (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Oraarch_sidlun	Ja.	Aus

ASM RAC-Datenbanken

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Orabin_Host namelun	Ja.	Ein
Datendateien	Oradata_sid	Oradata_sidlun	Ja.	Aus

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Temporäre Datendateien	Oratep_sid	Oratepp_sidlun	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Oracntrl01_sidlun (Multiplexed) Oracntrl02_sidlun (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Oralog01_dbnamelun (Multiplexed) Oralogen02_dbnamelun (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Oraarch_sidlun	Ja.	Aus
Cluster-Dateien	Oracrs_clustername	Oracrs_clusternamelun	Ja.	Ein

Einschränkungen bei der Arbeit mit SnapManager

Sie müssen die Szenarien und Einschränkungen kennen, die sich auf Ihre Umgebung auswirken können.

Einschränkungen im Zusammenhang mit Datenbank-Layouts und Plattformen

- SnapManager unterstützt Steuerdateien auf einem Dateisystem in einer ASM-Laufwerksgruppe und unterstützt keine Steuerdateien auf RAW-Geräten.
- SnapManager arbeitet in einer Microsoft Clustering-Umgebung (MSCS), erkennt jedoch den Status der MSCS-Konfiguration (aktiv oder passiv) nicht und überträgt kein aktives Management eines Repositorys in einen Standby-Server in einem MSCS-Cluster.
- In Red hat Enterprise Linux (RHEL) und Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 und 5.3 wird das ext3-Dateisystem bei der Bereitstellung von Oracle über RAW-Geräte durch Verwendung von dynamischem Multipathing (DMP) in einer Multipath Network I/O (MPIO)-Umgebung nicht unterstützt.

  Dieses Problem ist in SnapManager nur bemerkt, wenn SnapDrive 4.1 für UNIX oder frühere Versionen verwendet wird.

- SnapManager unter RHEL unterstützt die Partitionierung von Festplatten mit dem Dienstprogramm **parted** nicht.

  Dies ist ein Problem mit dem Dienstprogramm RHEL **parted**.

- Wenn in einer RAC-Konfiguration ein Profilname aus RAC-Knoten A aktualisiert wird, wird die Zeitplandatei für das Profil nur für RAC-Knoten A aktualisiert

  Die Zeitplandatei für dasselbe Profil auf RAC-Knoten B wird nicht aktualisiert und enthält die früheren

Terminplaninformationen. Wenn ein geplantes Backup von Knoten B ausgelöst wird, schlägt der geplante Backup-Vorgang fehl, da Node B die frühere Zeitplandatei enthält. Der geplante Sicherungsvorgang ist jedoch von Knoten A erfolgreich, auf dem das Profil umbenannt wird. Sie können den SnapManager-Server neu starten, sodass Sie die neueste Zeitplandatei für das Profil auf Knoten B. erhalten

- Die Repository-Datenbank kann auf einem Host vorhanden sein, auf den über mehrere IP-Adressen zugegriffen werden kann.

  Wenn über mehrere IP-Adressen auf das Repository zugegriffen wird, wird die Zeitplandatei für jede der IP-Adressen erstellt. Wenn die Backup-Planung für ein Profil (z. B. Profil A) unter einer der IP-Adressen (z. B. IP1) erstellt wird, wird die Zeitplandatei nur für diese IP-Adresse aktualisiert. Wenn von einer anderen IP-Adresse auf Profil A zugegriffen wird (z. B. IP2), wird das geplante Backup nicht aufgeführt, da die Terminplandatei von IP2 keinen Eintrag für den unter IP1 erstellten Zeitplan hat.

  Sie können warten, bis der Zeitplan von dieser IP-Adresse und der Zeitplandatei ausgelöst wird, oder Sie können den Server neu starten.

Einschränkungen in Bezug auf die SnapManager-Konfiguration

- SnapManager kann für die Katalogisierung von Datenbank-Backups mit RMAN konfiguriert werden.

  Wenn ein RMAN-Wiederherstellungskatalog verwendet wird, muss sich der Wiederherstellungskatalog in einer anderen Datenbank befinden als die gesicherte Datenbank.

- SnapDrive für UNIX unterstützt auf bestimmten Plattformen mehr als einen Filesystem- und Volume-Manager.

  Der für Datenbankdateien verwendete Dateisystem- und Volume-Manager muss in der SnapDrive-Konfigurationsdatei als Standarddateisystem und Volume Manager angegeben werden.

- SnapManager unterstützt Datenbanken auf MultiStore Storage-Systemen unter folgenden Anforderungen:
  - Sie müssen SnapDrive konfigurieren, um Passwörter für MultiStore Storage-Systeme festzulegen.
  - SnapDrive kann keine Snapshot Kopie einer LUN oder Datei in einem qtree in einem MultiStore Storage-System erstellen, wenn sich das zugrunde liegende Volume nicht im selben MultiStore Storage-System befindet.
- SnapManager unterstützt nicht den Zugriff auf zwei SnapManager Server, die auf verschiedenen Ports über einen einzelnen Client laufen (sowohl über CLI als auch über GUI).

  Die Port-Nummern sollten auf dem Ziel- und den Remote-Hosts identisch sein.

- Alle LUNs in einem Volume sollten auf Volume-Ebene oder in qtrees liegen, jedoch nicht beides.

  Das liegt daran, dass die Daten in den qtrees liegen und Sie das Volume mounten, dann sind die Daten in den qtrees nicht geschützt.

- SnapManager-Vorgänge schlagen fehl und Sie können nicht auf die GUI zugreifen, wenn die Repository-Datenbank ausfällt.

  Sie müssen überprüfen, ob die Repository-Datenbank ausgeführt wird, wenn Sie SnapManager-Vorgänge durchführen.

- SnapManager unterstützt keine Live Partition Mobility (LPM) und Live Application Mobility (LAM).
- SnapManager unterstützt Oracle Wallet Manager und Transparent Data Encryption (TDE) nicht.

- MetroCluster-Konfigurationen werden von SnapManager in RDM-Umgebungen (Raw Device Mapping) nicht unterstützt, da MetroCluster-Konfigurationen noch von der Virtual Storage Console (VSC) unterstützt werden müssen.

Einschränkungen im Zusammenhang mit der Profilverwaltung

- Wenn Sie das Profil aktualisieren, um die Backups des Archivprotokolls voneinander zu trennen, können Sie auf dem Host keinen Rollback-Vorgang durchführen.
- Wenn Sie ein Profil von der GUI aktivieren, um Archiv-Protokoll-Backups zu erstellen, und später versuchen, das Profil mithilfe des Fensters „Multi Profile Update“ oder des Fensters „Profile Update“ zu aktualisieren, können Sie dieses Profil nicht ändern, um ein vollständiges Backup zu erstellen.
- Wenn Sie im Fenster Multi Profile Update mehrere Profile aktualisieren und bei einigen Profilen die Option **Backup Archivilogs separat** aktiviert ist und andere Profile die Option deaktiviert haben, ist die Option **Archivprotokolle separat** sichern deaktiviert.
- Wenn Sie mehrere Profile aktualisieren und einige Profile die Option **Backup Archivilogs separat** aktivieren und andere Profile die Option deaktiviert haben, ist die Option **Backup Archivilogs separat** im Fenster Multi Profile Update deaktiviert.
- Wenn Sie das Profil umbenennen, können Sie den Host nicht zurückführen.

Einschränkungen im Zusammenhang mit Rolling Upgrade oder Rollback-Vorgängen

- Wenn Sie versuchen, eine frühere Version von SnapManager für einen Host zu installieren, ohne den Rollback-Vorgang auf dem Host im Repository durchzuführen, können Sie Folgendes möglicherweise nicht ausführen:
  - Sehen Sie sich die Profile an, die in früheren oder neueren Versionen von SnapManager für den Host erstellt wurden.
  - Greifen Sie auf Backups oder Klone zu, die in früheren oder neueren Versionen von SnapManager erstellt wurden.
  - Führen Sie Rolling Upgrade- oder Rollback-Vorgänge auf dem Host durch.
- Nachdem Sie die Profile getrennt haben, um Backups für Archivprotokolle zu erstellen, können Sie im zugehörigen Host Repository keinen Rollback-Vorgang durchführen.

Einschränkungen im Zusammenhang mit Backup-Vorgängen

- Die Backup-Erstellung kann fehlschlagen, wenn Sie SnapManager Vorgänge gleichzeitig auf demselben Host auf einer anderen ASM-Datenbank ausführen.
- Wenn der Backup während der Recovery bereits angehängt ist, mounted SnapManager den Backup nicht erneut und verwendet das bereits bereitgestellte Backup.

  Wenn das Backup von einem anderen Benutzer gemountet wird und Sie keinen Zugriff auf das zuvor bereitgestellte Backup haben, muss der andere Benutzer Ihnen die Berechtigung erteilen.

  Alle Archivprotokolldateien haben Leseberechtigung für Benutzer, die einer Gruppe zugewiesen sind. Sie haben möglicherweise nicht die Zugriffsberechtigung für die Archivprotokolldatei, wenn das Backup von einer anderen Benutzergruppe gemountet wird. Benutzer können die gemounteten Archivprotokolldateien manuell erteilen und den Wiederherstellungsvorgang oder die Wiederherstellung wiederholen.

- SnapManager legt den Backup-Status als „`PROTECTED`“ fest, selbst wenn eine der Snapshot-Kopien des Datenbank-Backups auf das sekundäre Storage-System übertragen wird.
- Sie können die Aufgabenspezifikationsdatei nur für geplante Backups aus SnapManager 3.2 oder höher

verwenden.

- Wenn ein Backup- oder Klonvorgang gleichzeitig auf den 10gR2- und 11gR2 RAC-Datenbanken über ASM ausgeführt wird, schlägt eine der Backup- oder Klonerstellung fehl.

  Dieser Fehler liegt an einer bekannten Oracle Einschränkung.

- SnapManager ist in den Protection Manager integriert und unterstützt das Backup mehrerer Volumes im Primärspeicher zu einem einzigen Volume im Sekundärspeicher von SnapVault und qtree SnapMirror.

  Die dynamische Dimensionierung eines sekundären Volumes wird nicht unterstützt. Weitere Informationen hierzu finden Sie im Provisioning Manager und Protection Manager – Administratorhandbuch für die Verwendung mit DataFabric Manager Server 3.8.

- SnapManager unterstützt mit dem Post-Processing-Skript nicht das Vaulting von Backups.
- Wenn die Repository-Datenbank auf mehr als eine IP-Adresse verweist und jede IP-Adresse einen anderen Hostnamen hat, ist der Backup-Planungsvorgang für eine IP-Adresse erfolgreich, schlägt aber für die andere IP-Adresse fehl.
- Nach einem Upgrade auf SnapManager 3.4 oder höher können alle mit Nachverarbeitungsskripten unter SnapManager 3.3.1 geplanten Backups nicht aktualisiert werden.

  Sie müssen den vorhandenen Zeitplan löschen und einen neuen Zeitplan erstellen.

Einschränkungen im Zusammenhang mit Wiederherstellungsvorgängen

- Wenn Sie eine indirekte Methode zur Durchführung eines Wiederherstellungsvorgangs verwenden und die für die Wiederherstellung erforderlichen Archivprotokolldateien nur bei Backups vom sekundären Speichersystem verfügbar sind, kann SnapManager die Datenbank nicht wiederherstellen.

  Der Grund dafür ist, dass SnapManager das Backup von Archivprotokolldateien nicht vom sekundären Storage-System mounten kann.

- Wenn SnapManager eine Volume-Wiederherstellung durchführt, werden die Backupkopien des Archivprotokolls, die nach der Wiederherstellung des entsprechenden Backups erstellt werden, nicht gelöscht.

  Wenn sich die Datendateien und das Ziel der Archivprotokolldatei auf demselben Volume befinden, können die Datendateien durch eine Wiederherstellung des Volumes wiederhergestellt werden, wenn im Ziel der Archivprotokolldatei keine Archivprotokolldateien vorhanden sind. In einem solchen Szenario gehen die Snapshot Kopien des Archivprotokolls verloren, die nach dem Backup der Dateien erstellt wurden.

  Sie sollten nicht alle Archivprotokolldateien vom Archivprotokollziel löschen.

- Wenn in einer ASM-Umgebung auf einer Laufwerksgruppe, die Datendateien hat, Oracle Cluster Registry (OCR) und Voting Disk-Dateien koexistieren, zeigt der Schnellwiederherstellungsvorgang die falsche Verzeichnisstruktur für den OCR- und Voting-Datenträger an.

Einschränkungen im Zusammenhang mit Klonvorgängen

- Aufgrund der Geschwindigkeit, mit der die Inodes vom Speichersystem erkannt und verarbeitet werden, das das flexible Volume enthält, können Sie keine numerischen Werte zwischen 0 und 100 für den Fortschritt des Clone-Split-Vorgangs anzeigen.
- SnapManager unterstützt nicht das Empfangen von E-Mails nur für erfolgreiche Klontrennvorgänge.

- SnapManager unterstützt nur die Aufteilung eines FlexClone.
- Das Klonen des Online-Datenbank-Backups der RAC-Datenbank, die den Speicherort der externen Archivprotokolldatei verwendet, ist aufgrund eines Fehlers bei der Wiederherstellung fehlgeschlagen.

  Das Klonen schlägt fehl, da Oracle die Archivprotokolldateien nicht für die Wiederherstellung vom externen Archivprotokollspeicherort findet und angewendet. Dies ist eine Einschränkung von Oracle. Weitere Informationen finden Sie unter Oracle Bug ID: 13528007. Oracle wendet Archivprotokoll nicht vom nicht standardmäßigen Speicherort auf dem an "Oracle Support Website". Sie müssen über einen gültigen Oracle metalink-Benutzernamen und ein gültiges Kennwort verfügen.

- SnapManager 3.3 oder höher unterstützt nicht mit der XML-Datei für die Klonspezifikation, die in den Versionen vor SnapManager 3.2 erstellt wurde.
- Wenn sich temporäre Tablespaces an einem anderen Speicherort als dem Datendateien befinden, erstellt ein Klonvorgang die Tabellen im Datendateien.

  Wenn jedoch temporäre Tablespaces Oracle Managed Files (OMFs) sind, die sich an einem anderen Speicherort als dem Datendateien befinden, erstellt der Klonvorgang nicht die Tabellen im Datendateien. Die OMFs werden nicht von SnapManager verwaltet.

- SnapManager kann eine RAC Datenbank nicht klonen, wenn Sie die Option -resetlogs auswählen.

Einschränkungen im Zusammenhang mit Archiv-Log-Dateien und Backups

- SnapManager unterstützt keine Anschnitt von Archiv-Log-Dateien aus dem Flash-Recovery-Bereich Ziel.
- SnapManager unterstützt nicht das Aufheben von Archivprotokolldateien vom Standby-Ziel.
- Die Backups für das Archivprotokoll werden basierend auf der Aufbewahrungsdauer und der standardmäßigen stündlichen Aufbewahrungsklasse beibehalten.

  Wenn die Klasse für die Backup-Aufbewahrung des Archivprotokolls über die SnapManager Befehlszeilenschnittstelle oder Benutzeroberfläche geändert wird, gilt die geänderte Aufbewahrungsklasse nicht für das Backup, da die Backups des Archivprotokolls basierend auf der Aufbewahrungsdauer aufbewahrt werden.

- Wenn Sie die Archivprotokolldateien aus den Zielen des Archivprotokolls löschen, enthält die Backup des Archivprotokolls keine Archivprotokolldateien, die älter sind als die fehlende Archivprotokolldatei.

  Wenn die letzte Archivprotokolldatei fehlt, schlägt die Sicherung des Archivprotokolls fehl.

- Wenn Sie die Archivprotokolldateien aus den Archivprotokollzielen löschen, schlägt das Beschneiden von Archivprotokolldateien fehl.
- SnapManager konsolidiert die Archiv-Log-Backups, selbst wenn Sie die Archiv-Log-Dateien aus den Archiv-Log-Zielen löschen oder wenn die Archiv-Log-Dateien beschädigt sind.

Einschränkungen im Zusammenhang mit der Änderung des Host-Namens der Zieldatenbank

Die folgenden SnapManager Vorgänge werden nicht unterstützt, wenn Sie den Host-Namen der Zieldatenbank ändern:

- Ändern des Host-Namens der Zieldatenbank von der SnapManager-GUI.
- Rollback der Repository-Datenbank nach Aktualisierung des Host-Namens der Zieldatenbank des Profils durchführen.
- Gleichzeitige Aktualisierung mehrerer Profile für einen neuen Hostnamen der Zieldatenbank.

- Ändern des Host-Namens der Zieldatenbank, wenn ein SnapManager-Vorgang ausgeführt wird.

Einschränkungen im Zusammenhang mit der SnapManager CLI oder GUI

- Die CLI-Befehle von SnapManager für den Vorgang zum Erstellen von Profilen, die über die Benutzeroberfläche von SnapManager generiert werden, verfügen über keine Optionen zur Verlaufskonfiguration.

  Mit dem Befehl „Profile create“ können Sie die Verlaufs-Aufbewahrungseinstellungen über die SnapManager-CLI konfigurieren.

- SnapManager zeigt die GUI in Mozilla Firefox nicht an, wenn auf dem UNIX-Client keine Java Runtime Environment (JRE) verfügbar ist.
- Wenn beim Aktualisieren des Host-Namens der Zieldatenbank mithilfe der SnapManager CLI eine oder mehrere offene SnapManager GUI-Sitzungen vorliegen, reagieren nicht alle offenen SnapManager GUI-Sitzungen.

Einschränkungen im Zusammenhang mit SnapMirror und SnapVault

- Das SnapVault Post-Processing-Skript wird nicht unterstützt, wenn Sie Data ONTAP 7-Mode verwenden.
- Wenn Sie ONTAP verwenden, können Sie Volume-basierte SnapRestore (VBSR) nicht auf den Backups ausführen, die in den Volumes erstellt wurden, über die SnapMirror Beziehungen festgelegt sind.

  Dies liegt an einer ONTAP Einschränkung, die es Ihnen nicht erlaubt, die Beziehung bei der Durchführung einer VBSR zu unterbrechen. Sie können jedoch eine VBSR beim letzten oder kürzlich erstellten Backup nur ausführen, wenn die Volumes SnapVault Beziehungen eingerichtet haben.

- Wenn Sie Data ONTAP in 7-Mode verwenden und eine VBSR für die Backups ausführen möchten, die in den Volumes erstellt wurden, auf denen SnapMirror Beziehungen festgelegt sind, können Sie die Option override-vbsr-snapmirror-Check in SnapDrive für UNIX auf ON setzen.

  Weitere Informationen dazu finden Sie in der SnapDrive-Dokumentation.

- In einigen Szenarien können Sie das letzte Backup, das mit der ersten Snapshot Kopie verbunden ist, nicht löschen, wenn das Volume eine SnapVault-Beziehung eingerichtet hat.

  Sie können das Backup nur löschen, wenn Sie die Beziehung unterbrechen. Dieses Problem liegt an einer ONTAP-Einschränkung bei Basis-Snapshot-Kopien. In einer SnapMirror Beziehung wird die Snapshot Basiskopie von der SnapMirror Engine erstellt und in einer SnapVault Beziehung ist die Snapshot Basiskopie das Backup, das mit SnapManager erstellt wurde. Die Basis-Snapshot-Kopie verweist bei jedem Update auf das neueste Backup, das mithilfe von SnapManager erstellt wird.

Einschränkungen im Zusammenhang mit Data Guard Standby-Datenbanken

- SnapManager unterstützt keine Standby-Datenbanken für die logische Datenwache.
- SnapManager unterstützt keine Standby-Datenbanken für Active Data Guard.
- SnapManager erlaubt keine Online-Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine partiellen Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt nicht die Wiederherstellung von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine Beschneidung von Archivprotokolldateien für Data Guard Standby-Datenbanken.

- SnapManager unterstützt den Broker nicht.

Verwandte Informationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

SnapManager Limitierungen für Clustered Data ONTAP

Sie müssen die Einschränkungen für einige Funktionalitäten und SnapManager-Vorgänge kennen, wenn Sie Clustered Data ONTAP verwenden.

Die folgenden Funktionalitäten werden nicht unterstützt, wenn Sie SnapManager auf Clustered Data ONTAP nutzen:

- Datensicherungsfunktionen, wenn SnapManager in OnCommand Unified Manager integriert ist
- Eine Datenbank, in der eine LUN zu einem System gehört, auf dem Data ONTAP 7-Mode und die andere LUN ausgeführt werden, gehört zu einem System mit Clustered Data ONTAP
- SnapManager für Oracle unterstützt keine Migration von Vserver, wie sie von Clustered Data ONTAP nicht unterstützt wird
- SnapManager für Oracle unterstützt die Funktion Clustered Data ONTAP 8.2.1 nicht zur Festlegung verschiedener Exportrichtlinien für Volumes und qtrees

Einschränkungen in Bezug auf Oracle Database

Bevor Sie mit der Arbeit mit SnapManager beginnen, müssen Sie die Einschränkungen in Bezug auf Oracle Database kennen.

Die Einschränkungen sind wie folgt:

- SnapManager unterstützt Oracle Versionen 10gR2, 11gR1, 11gR2 und 12*c*, unterstützt aber Oracle 10gR1 als Repository oder Zieldatenbank nicht.
- SnapManager unterstützt die Verwendung einer SCAN-IP-Adresse anstelle eines Hostnamens nicht.

  SCAN-IP ist eine neue Funktion in Oracle 11gR2.

- Oracle Cluster File System (OCFS) wird von SnapManager nicht unterstützt.
- Oracle 11g in einer Direct NFS-Umgebung (dNFS) ermöglicht zusätzliche Mount-Point-Konfigurationen in der oranfstab-Datei, z. B. mehrere Pfade für den Lastausgleich.

  SnapManager ändert die oranfstab-Datei nicht. Sie müssen in der oranfstab-Datei manuell weitere Eigenschaften hinzufügen, die die geklonte Datenbank verwenden soll.

- Unterstützung für Oracle Database 9i ist veraltet aus SnapManager 3.2.
- Der Support für Oracle Database 10gR2 (früher als 10.2.0.5) ist veraltet aus SnapManager 3.3.1.

Ermitteln Sie die verschiedenen Versionen von Oracle Datenbanken, die durch die Interoperabilitäts-Matrix unterstützt werden.

Verwandte Informationen

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Veraltete Versionen der Oracle-Datenbank

Oracle Database 9i wird von SnapManager 3.2 oder höher nicht unterstützt, und die Oracle Database 10gR2 (früher als 10.2.0.4) wird von SnapManager 3.3.1 oder höher nicht unterstützt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und auf SnapManager 3.2 oder höher aktualisieren möchten, können Sie keine neuen Profile erstellen. Eine Warnmeldung wird angezeigt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und ein Upgrade auf SnapManager 3.2 oder höher durchführen möchten, müssen Sie eine der folgenden Aktionen durchführen:

- Aktualisieren Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken auf entweder Oracle 10gR2 (10.2.0.5), 11gR1 oder 11gR2 Datenbanken und führen Sie ein Upgrade auf SnapManager 3.2 oder 3.3 durch.

  Wenn Sie ein Upgrade auf Oracle 12*c* durchführen, müssen Sie ein Upgrade auf SnapManager 3.3.1 oder höher durchführen.

  Oracle Datenbank 12*c* wird nur von SnapManager 3.3 unterstützt.

- Verwalten Sie die Oracle 9i-Datenbanken mit einer Patch-Version von SnapManager 3.1.

  Sie können SnapManager 3.2 oder 3.3 verwenden, wenn Sie Oracle 10gR2-, 11gR1- oder 11gR2-Datenbanken verwalten und SnapManager 3.3.1 oder höher verwenden möchten, wenn Sie Oracle 12*c* -Datenbanken zusammen mit anderen unterstützten Datenbanken verwalten möchten.

Einschränkungen beim Volume-Management

Bei SnapManager gibt es bestimmte Volume-Management-Einschränkungen, die sich auf Ihre Umgebung auswirken können.

Sie können mehrere Laufwerksgruppen für eine Datenbank haben. Die folgenden Einschränkungen gelten jedoch für alle Festplattengruppen für eine bestimmte Datenbank:

- Plattengruppen für die Datenbank können nur von einem Volume-Manager verwaltet werden.
- Von einem logischen Volume-Manager gesicherte RAW-Geräte werden für den Schutz von Oracle Daten nicht unterstützt.

  RAW Device Storage und Automatic Storage Management (ASM)-Festplattengruppen müssen direkt auf physischen Geräten bereitgestellt werden. In einigen Fällen ist eine Partitionierung erforderlich.

- Eine Linux-Umgebung ohne logisches Volume-Management erfordert eine Partition.

Backups mit Snapshot Kopien erstellen

Mit SnapManager können Sie Backups auf dem primären (lokalen) Storage und auch auf dem sekundären (Remote-) Storage mithilfe von Sicherungsrichtlinien oder Nachbearbeitungsskripten erstellen.

Als Snapshot-Kopien erstellte Backups sind virtuelle Kopien der Datenbank und werden auf demselben

physischen Medium wie die Datenbank gespeichert. Der Backup-Vorgang dauert daher weniger Zeit und erfordert deutlich weniger Speicherplatz als vollständige Disk-to-Disk Backups. Mit SnapManager können Sie Folgendes sichern:

- Alle Datendateien, archivierte Log-Dateien und Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces, alle Archivprotokolldateien und Kontrolldateien

Mit SnapManager 3.2 oder höher können Sie optional folgende Daten sichern:

- Alle Datendateien und die Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces zusammen mit den Kontrolldateien
- Archivierung von Protokolldateien

Die Datendateien, Archiv-Log-Dateien und Kontrolldateien können auf verschiedenen Storage-Systemen, Storage-System-Volumes oder LUNs (Logical Unit Numbers) abgelegt werden. Sie können SnapManager auch zum Backup einer Datenbank verwenden, wenn sich mehrere Datenbanken auf demselben Volume oder LUN befinden.

Warum sollten Sie Archiv Log-Dateien beschneiden

Mit SnapManager für Oracle können Sie Archivprotokolldateien aus dem aktiven, bereits gesicherten Dateisystem löschen.

Durch Beschneidung kann SnapManager Backups einzelner Archiv-Log-Dateien erstellen. Durch Beschneidung und die Richtlinie zur Aufbewahrung von Backups wird beim Säuberen von Backups der Speicherplatz für das Archiv-Protokoll freigegeben.

Sie können die Archivprotokolldateien nicht beschneiden, wenn der Flash Recovery Area (FRA) für Archivprotokolldateien aktiviert ist. Wenn Sie im Bereich Flash Recovery den Speicherort für das Archivprotokoll angeben, müssen Sie im Parameter Archive_log_dest auch den Speicherort für das Archivprotokoll angeben.

Konsolidierung von Archivierungsprotokolldaten

Mit SnapManager (3.2 oder höher) für Oracle werden die Archiv-Log-Backups konsolidiert, um eine Mindestanzahl an Backups für Archivierungs-Log-Dateien beizubehalten. SnapManager für Oracle erkennt und befreit die Backups, die Archivprotokolle enthalten, die Teilmengen anderer Backups sind.

Vollständige oder teilweise Wiederherstellung von Datenbanken

SnapManager bietet die Flexibilität, komplette Datenbanken, bestimmte Tabellen, Dateien, Kontrolldateien oder eine Kombination dieser Einheiten wiederherzustellen. SnapManager ermöglicht die Wiederherstellung von Daten mithilfe eines dateibasierten Wiederherstellungsprozesses mit einem schnelleren, Volume-basierten Wiederherstellungsprozess. Datenbankadministratoren können den Prozess auswählen,

den sie verwenden möchten, oder SnapManager entscheiden lassen, welcher Prozess für Sie geeignet ist.

SnapManager ermöglicht Datenbankadministratoren (DBAs) die Vorschau von Restore-Vorgängen. Mit der Vorschaufunktion können DBAs jeden Wiederherstellungsvorgang auf Datei-für-Datei-Basis anzeigen.

Datenbankadministratoren können das Level angeben, auf das SnapManager bei der Durchführung von Restore-Vorgängen wiederhergestellt und Informationen wiederhergestellt werden. Beispielsweise können DBAs Daten zu bestimmten Zeitpunkten wiederherstellen. Der Wiederherstellungspunkt kann ein Datum und eine Uhrzeit oder eine Oracle System Change Number (SCN) sein.

Datenbankadministratoren können die Datenbank mit SnapManager wiederherstellen und ein anderes Tool verwenden, um die Informationen wiederherzustellen. DBAs müssen für beide Vorgänge keine SnapManager verwenden.

Mit SnapManager (3.2 oder höher) können Datenbank-Backups automatisch und ohne Eingriff des Datenbankadministrators wiederhergestellt werden. Sie können SnapManager verwenden, um Backups für Archivprotokolle zu erstellen und dann diese Backups für Archivprotokolle zu verwenden, um die Datenbank-Backups wiederherzustellen und wiederherzustellen. Selbst wenn die Archivprotokolldateien des Backups in einem externen Archivprotokoll verwaltet werden, können Sie diesen externen Speicherort angeben, damit diese Archivprotokolle zur Wiederherstellung der wiederhergestellten Datenbank beitragen können.

Überprüfen des Backup-Status

SnapManager kann die Integrität des Backups mithilfe von standardmäßigen Oracle-Backup-Verifizierungsvorgängen bestätigen.

Datenbankadministratoren (DBAs) können die Verifizierung im Rahmen des Backup-Vorgangs oder einer anderen Zeit durchführen. Datenbankadministratoren können den Verifizierungsvorgang so einstellen, dass er bei geringerer Auslastung des Host-Servers oder während eines geplanten Wartungsfensters ausgeführt wird.

Datenbank-Backup-Klone

SnapManager erstellt mithilfe der FlexClone Technologie einen beschreibbaren, platzsparenden Klon eines Datenbank-Backups. Sie können einen Klon ändern, ohne die Backup-Quelle zu ändern.

Möglicherweise möchten Sie Datenbanken klonen, um Tests oder Upgrades in nicht produktiven Umgebungen zu ermöglichen. Sie können eine Datenbank mit einem primären oder sekundären Storage klonen. Ein Klon kann sich auf demselben Host oder einem anderen Host befinden wie die Datenbank.

Mit der FlexClone Technologie können SnapManager Snapshot-Kopien der Datenbank verwenden, sodass keine vollständige physische Disk-to-Disk-Kopie erstellt werden muss. Snapshot Kopien benötigen weniger Erstellungszeit und belegen deutlich weniger Speicherplatz als physische Kopien.

In der Data ONTAP Dokumentation finden Sie weitere Informationen zur FlexClone Technologie.

Verwandte Informationen

"Data ONTAP documentation: mysupport.netapp.com/documentation/productsatoz/index.html"

Verfolgen Sie die Details und erstellen Sie Berichte

SnapManager bietet nicht nur detaillierte Datenbankadministratoren, die den Status verschiedener Vorgänge verfolgen müssen, sondern mithilfe von Methoden, die Vorgänge über eine einheitliche Benutzeroberfläche überwachen.

Nachdem Administratoren festlegen, welche Datenbanken gesichert werden sollen, identifiziert SnapManager die Datenbankdateien für das Backup automatisch. SnapManager zeigt Informationen zu Repositorys, Hosts, Profilen, Backups und Klonen an. Sie können die Vorgänge auf bestimmten Hosts oder Datenbanken überwachen.Sie können auch die geschützten Backups identifizieren und bestimmen, ob die Backups in Bearbeitung sind oder geplant werden.

Repositories

SnapManager organisiert die Informationen in Profile, die dann den Repositories zugeordnet werden. Profile enthalten Informationen über die zu verwaltende Datenbank, während das Repository Daten zu den Vorgängen enthält, die auf Profilen ausgeführt werden.

Das Repository zeichnet auf, wann ein Backup durchgeführt wurde, welche Dateien gesichert wurden und ob ein Klon aus dem Backup erstellt wurde. Wenn Datenbankadministratoren eine Datenbank wiederherstellen oder einen Teil davon wiederherstellen, fragt SnapManager das Repository ab, um zu ermitteln, was gesichert wurde.

Da das Repository die Namen der während des Backup erstellten Datenbank-Snapshot-Kopien speichert, kann die Repository-Datenbank nicht in derselben Datenbank vorhanden sein und kann auch nicht Teil derselben Datenbank sein, die von SnapManager gesichert wird. Sie müssen mindestens zwei Datenbanken (die SnapManager Repository-Datenbank und die von SnapManager gemanagte Zieldatenbank) einrichten und ausführen, wenn Sie SnapManager Vorgänge ausführen.

Wenn Sie versuchen, die grafische Benutzeroberfläche (GUI) zu öffnen, wenn die Repository-Datenbank nicht verfügbar ist, wird die folgende Fehlermeldung in der Datei sm_gui.log protokolliert: [WARNUNG]: SMO-01106: Beim Abfragen des Repository ist ein Fehler aufgetreten: Keine Daten mehr aus dem Socket zu lesen. Außerdem schlägt das SnapManager-Verfahren fehl, wenn die Repository-Datenbank ausfällt. Weitere Informationen zu den verschiedenen Fehlermeldungen finden Sie unter *Fehlerbehebung bekannter Probleme*.

Sie können jeden beliebigen Host-Namen, Dienstnamen oder Benutzernamen verwenden, um Vorgänge auszuführen. Damit ein Repository SnapManager-Vorgänge unterstützt, müssen der Projektarchiv-Benutzername und der Dienstname nur aus den folgenden Zeichen bestehen: Alphabetische Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-), Unterstrich (_) und Punkt (.).

Der Repository-Port kann eine beliebige gültige Portnummer sein, und der Repository-Hostname kann einen beliebigen gültigen Hostnamen sein. Der Hostname muss aus alphabetischen Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-) und Periode (.) bestehen, jedoch nicht aus einem Unterstrich (_).

Das Repository muss in einer Oracle-Datenbank erstellt werden. Die von SnapManager verwendete Datenbank sollte gemäß den Oracle Verfahren für die Datenbankkonfiguration eingerichtet werden.

Ein einziges Repository kann Informationen über mehrere Profile enthalten, jedoch ist jede Datenbank normalerweise nur mit einem Profil verknüpft. Sie können mehrere Repositorys haben, wobei jedes Repository mehrere Profile enthält.

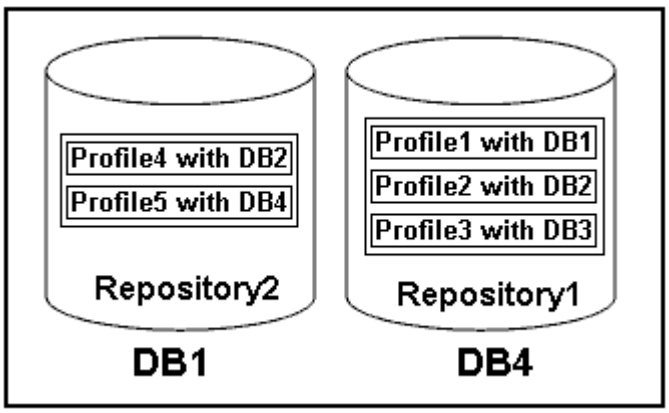
Welche Profile sind

SnapManager verwendet Profile, um die zur Durchführung von Operationen in einer bestimmten Datenbank erforderlichen Informationen zu speichern. Ein Profil enthält die Informationen zur Datenbank einschließlich aller Anmeldeinformationen, Backups und Klone. Wenn Sie ein Profil erstellen, müssen Sie keine Datenbankdetails angeben, wenn Sie eine Operation in dieser Datenbank ausführen.

Ein Profil kann nur auf eine Datenbank verweisen. Auf dieselbe Datenbank kann mit mehr als einem Profil verwiesen werden. Auf Backups, die mit einem Profil erstellt werden, kann nicht über ein anderes Profil zugegriffen werden, auch wenn beide Profile auf dieselbe Datenbank verweisen.

Profilinformationen werden in einem Repository gespeichert. Das Repository enthält sowohl die Profilinformationen für die Datenbank als auch Informationen zu den Snapshot-Kopien, die als Datenbank-Backup dienen. Die tatsächlichen Snapshot Kopien werden im Storage-System gespeichert. Die Namen der Snapshot Kopie werden im Repository gespeichert, das das Profil für diese Datenbank enthält. Wenn Sie einen Vorgang in einer Datenbank ausführen, müssen Sie das Profil aus dem Repository auswählen.

Die folgende Abbildung zeigt, wie Repositories mehrere Profile aufnehmen können, aber auch dass jedes Profil nur eine Datenbank definieren kann:



Im vorhergehenden Beispiel befindet sich Repository2 auf Datenbank DB1 und Repository1 befindet sich auf der Datenbank DB4.

Jedes Profil enthält die Anmeldeinformationen für die Datenbank, die mit dem Profil verknüpft ist. Mit den Anmeldeinformationen kann SnapManager eine Verbindung zur Datenbank herstellen und mit der Datenbank arbeiten. Die gespeicherten Anmeldeinformationen umfassen den Benutzernamen und die Kennwortpaare für den Zugriff auf den Host, das Repository, die Datenbank und die erforderlichen Verbindungsinformationen, wenn Sie Oracle Recovery Manager (RMAN) verwenden.

Sie können nicht auf ein Backup zugreifen, das mit einem Profil aus einem anderen Profil erstellt wurde, auch wenn beide Profile mit derselben Datenbank verknüpft sind. SnapManager legt eine Sperre auf die Datenbank ab, um zu verhindern, dass zwei inkompatible Vorgänge gleichzeitig ausgeführt werden.

Profil zur Erstellung vollständiger und partieller Backups

Sie können Profile erstellen, um vollständige Backups oder partielle Backups zu erstellen.

Die Profile, die Sie zur Erstellung der vollständigen und partiellen Backups angeben, enthalten sowohl die Datendateien als auch die Archivprotokolldateien. SnapManager erlaubt solche Profile nicht, die Backups des

Archivprotokolls von den Backups der Datendatei zu trennen. Die vollständigen und teilweisen Backups werden basierend auf den vorhandenen Richtlinien zur Backup-Aufbewahrung aufbewahrt und basierend auf den vorhandenen Sicherungsrichtlinien geschützt. Sie können vollständige und teilweise Backups basierend auf der zu Ihnen passt Uhrzeit und Häufigkeit planen.

Profile für die Erstellung von datenbasierten Backups und nur-Archiv-Backups

Mit SnapManager (3.2 oder höher) können Sie Profile erstellen, die Backups der Archivprotokolldateien getrennt von den Datendateien machen. Nachdem Sie das Profil zur Trennung der Backup-Typen verwendet haben, können Sie entweder Datendateien-only-Backups oder lediglich Archiv-Log-Backups der Datenbank erstellen. Sie können auch ein Backup erstellen, das sowohl die Datendateien als auch die Archivprotokolldateien enthält.

Die Aufbewahrungsrichtlinie gilt für alle Datenbank-Backups, wenn die Archiv-Log-Backups nicht getrennt sind. Nachdem Sie die Backups für das Archivprotokoll getrennt haben, können Sie in SnapManager unterschiedliche Aufbewahrungszeiträume und Sicherungsrichtlinien für die Backups des Archivierungsprotokolls festlegen.

Aufbewahrungsrichtlinie

SnapManager legt fest, ob ein Backup aufbewahrt werden soll, indem sowohl die Anzahl der Aufbewahrung (z. B. 15 Backups) als auch die Aufbewahrungsdauer (z. B. 10 Tage tägliche Backups) berücksichtigt werden. Ein Backup läuft ab, wenn sein Alter die für seine Aufbewahrungsklasse festgelegte Aufbewahrungsdauer überschreitet und die Anzahl der Backups die Anzahl der Backups übersteigt. Beispiel: Wenn die Backup-Anzahl 15 beträgt (was bedeutet, dass SnapManager 15 erfolgreiche Backups erstellt hat) und die Dauer für tägliche Backups von 10 Tagen festgelegt wurde, verfallen die fünf ältesten, erfolgreichen und infrage kommenden Backups.

Aufbewahrungsdauer des Archivprotokolls

Nach Trennung der Backup-Protokolle werden sie basierend auf der Aufbewahrungsdauer des Archivprotokolls aufbewahrt. Backups von Archivprotokolldateien, die mit Backups von Datendateien erstellt werden, werden immer zusammen mit Backups dieser Datendateien aufbewahrt, unabhängig von der Aufbewahrungsdauer für das Archivprotokoll.

Verwandte Informationen

Profilverwaltung für effiziente Backups

Die Status der SnapManager-Operation lauten

SnapManager-Vorgänge (Backup, Wiederherstellung und Klon) können den jeweiligen Status aufweisen, wobei jeder Status den Fortschritt des Vorgangs angibt.

Betriebsstatus	Beschreibung
Erfolgreich	Die Operation wurde erfolgreich abgeschlossen.
Wird Ausgeführt	Der Vorgang wurde gestartet, ist aber noch nicht abgeschlossen. Ein Backup, das zwei Minuten dauert, wird beispielsweise um 11:00 Uhr morgens erstellt. Wenn Sie die Registerkarte **Zeitplan** um 11:01 Uhr aufrufen, wird der Vorgang als ausgeführt angezeigt.

Betriebsstatus	Beschreibung
Kein Vorgang gefunden	Der Zeitplan wurde nicht ausgeführt oder das letzte Backup wurde gelöscht.
Fehlgeschlagen	Der Vorgang ist fehlgeschlagen. SnapManager hat den Abbruchvorgang automatisch ausgeführt und den Vorgang bereinigt. **Hinweis:** Sie können den erstellten Klon teilen. Wenn Sie den geteilten Klon-Vorgang beenden, den Sie gestartet haben und der Vorgang erfolgreich angehalten wurde, wird der Status des Klon-Split-Vorgangs als fehlgeschlagen angezeigt.

Wiederherstellbare und nicht wiederherstellbare Ereignisse

Ein wiederherstellbares SnapManager Ereignis hat die folgenden Probleme:

- Die Datenbank wird nicht auf einem Storage-System gespeichert, auf dem Data ONTAP ausgeführt wird.
- Eine ASM-Datenbank (Automatic Storage Management) wird konfiguriert, die ASM-Instanz wird jedoch nicht ausgeführt.
- SnapDrive für UNIX ist nicht installiert oder kann nicht auf das Speichersystem zugreifen.
- SnapManager erstellt keine Snapshot Kopie bzw. stellt keinen Storage bereit, wenn das Volume über keinen freien Speicherplatz verfügt, die maximale Anzahl an Snapshot Kopien erreicht oder eine unerwartete Ausnahme auftritt.

Wenn ein wiederherstellbares Ereignis eintritt, wird SnapManager abgebrochen und versucht, den Host, die Datenbank und das Storage-System auf den Startstatus zurückzusetzen. Schlägt der Abbruchvorgang fehl, behandelt SnapManager den Vorfall als nicht wiederherstellbares Ereignis.

Wenn eines der folgenden Ereignisse eintritt, tritt ein nicht behebbares (Out-of-Band)-Ereignis auf:

- Ein Systemproblem tritt auf, z. B. wenn ein Host ausfällt.
- Der SnapManager-Prozess wird angehalten.
- Der Abbruch innerhalb des Band schlägt fehl, wenn das Speichersystem ausfällt, die Nummer der logischen Einheit (LUN) oder das Speichervolume offline ist oder das Netzwerk ausfällt.

Wenn ein nicht behebbares Ereignis eintritt, wird SnapManager sofort abgebrochen. Der Host, die Datenbank und das Speichersystem sind möglicherweise nicht an den ursprünglichen Status zurückgekehrt. In diesem Fall müssen Sie nach Ausfall des SnapManager-Vorgangs eine Bereinigung durchführen, indem Sie die verwaiste Snapshot Kopie löschen und die SnapManager-Sperrdatei entfernen.

Wenn Sie die SnapManager-Sperrdatei löschen möchten, navigieren Sie auf dem Zielcomputer zu Oracle_HOME €und löschen Sie die Datei SM_Lock_TargetDBName. Nach dem Löschen der Datei müssen Sie den SnapManager für Oracle-Server neu starten.

Wie SnapManager die Sicherheit gewährleistet

Sie können SnapManager Vorgänge nur ausführen, wenn Sie die entsprechenden Anmeldedaten besitzen. Die Sicherheit in SnapManager unterliegt der

Benutzerauthentifizierung und der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC). RBAC ermöglicht Datenbankadministratoren die Einschränkung von Vorgängen, die SnapManager auf den Volumes und LUNs ausführen kann, die die Datendateien in einer Datenbank enthalten.

Datenbankadministratoren ermöglichen die rollenbasierte Zugriffssteuerung für SnapManager mithilfe von SnapDrive. Datenbankadministratoren weisen anschließend SnapManager-Rollen Berechtigungen zu und weisen diese Rollen den Benutzern in der grafischen Benutzeroberfläche (GUI) oder der Befehlszeilenschnittstelle (CLI) von Operations Manager zu. RBAC-Berechtigungsprüfungen erfolgen im DataFabric Manager Server.

Zusätzlich zum rollenbasierten Zugriff behält SnapManager die Sicherheit bei, indem er die Benutzerauthentifizierung über Passwortaufforderungen oder die Festlegung von Benutzeranmeldeinformationen anfordert. Ein effektiver Benutzer wird beim SnapManager-Server authentifiziert und autorisiert.

Die SnapManager Anmeldedaten und die Benutzerauthentifizierung unterscheiden sich erheblich von SnapManager 3.0:

- In SnapManager-Versionen vor 3.0 würden Sie bei der Installation von SnapManager ein willkürliches Serverkennwort festlegen. Wer den SnapManager-Server nutzen möchte, braucht das SnapManager-Server-Passwort. Das SnapManager-Server-Passwort muss den Benutzeranmeldeinformationen mit dem smo-Befehl „set-serm“ hinzugefügt werden.
- In SnapManager (3.0 und höher) wurde das SnapManager-Serverpasswort durch die Authentifizierung des individuellen Betriebssystems (OS) ersetzt. Wenn Sie den Client nicht vom selben Server wie den Host ausführen, führt der SnapManager-Server die Authentifizierung durch, indem Sie die Benutzernamen und Passwörter des Betriebssystems verwenden. Wenn Sie nicht zur Eingabe Ihrer OS-Passwörter aufgefordert werden möchten, können Sie die Daten unter Verwendung des Befehls smo cridential set -Host im SnapManager-Benutzeranmeldungs-Cache speichern.

> Der Befehl smo Anmeldeinformation set -Host speichert Ihre Anmeldeinformationen, wenn die Eigenschaft Host.anmeldungs.persist in der Datei smo.config auf true gesetzt ist.

Beispiel

Benutzer1 und User2 teilen sich ein Profil namens Prof2. User2 kann eine Sicherung von „database1“ in Host1 nicht ohne die Berechtigung zum Zugriff auf Host1 durchführen. User1 kann eine Datenbank nicht ohne Berechtigung zum Zugriff auf host3 klonen.

In der folgenden Tabelle werden die verschiedenen Berechtigungen beschrieben, die den Benutzern zugewiesen sind:

Berechtigungstyp	Benutzer1	Benutzer2
Host-Passwort	Host1, Host2	Host2, Host3
Repository-Kennwort	Repos. 1	Repos. 1
Profilkennwort	Prof1, Prof2	Prof2

Wenn User1 und User2 keine freigegebenen Profile haben, nimmt an, dass User1 Berechtigungen für die

Hosts mit Namen Host1 und Host2 hat, und User2 hat Berechtigungen für den Host namens Host2. User2 kann nicht einmal die nicht-profilbefehlen wie dump und System verify auf Host1 ausführen.

Online-Hilfe aufrufen und drucken

Die Online-Hilfe enthält Anweisungen zu den Aufgaben, die Sie über die grafische Benutzeroberfläche von SnapManager ausführen können. Die Online-Hilfe enthält auch Beschreibungen der Felder in den Fenstern und Assistenten.

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Hauptfenster auf **Hilfe** > **Hilfe Inhalt**.
   - Klicken Sie in einem beliebigen Fenster oder Assistenten auf **Hilfe**, um Hilfe für dieses Fenster anzuzeigen.
2. Verwenden Sie das **Inhaltsverzeichnis** im linken Fensterbereich, um durch die Themen zu navigieren.
3. Klicken Sie oben im Hilfefenster auf das Druckersymbol, um einzelne Themen zu drucken.

Empfohlene allgemeine Datenbanklayouts und Speicherkonfigurationen

Durch das Wissen der empfohlenen allgemeinen Datenbank-Layouts und Storage-Konfigurationen können Sie Probleme in Bezug auf Festplattengruppen, Dateitypen und Tablespaces vermeiden.

- Fügen Sie keine Dateien aus mehr als einem SAN-Dateisystem oder Volume-Manager in Ihre Datenbank ein.

  Alle Dateien, die eine Datenbank erstellen, müssen sich auf demselben Dateisystem befinden.

- SnapManager erfordert mehrere 4 KB Blockgröße.
- Fügen Sie die Datenbank-System-ID in die oratab-Datei ein.

  Fügen Sie für jede zu verwaltende Datenbank einen Eintrag in die Oratab-Datei ein. SnapManager verlässt sich darauf, dass die oratab-Datei das Zuhause von Oracle bestimmt.

- Wenn Sie SnapManager-Backups mit dem Oracle Recovery Manager (RMAN) registrieren möchten, müssen Sie RMAN-fähige Profile erstellen.

Wenn Sie die neue Volume-basierte Wiederherstellung oder vollständige Laufwerksgruppenswiederherstellung nutzen möchten, sollten Sie die folgenden Richtlinien in Bezug auf Dateisysteme und Laufwerksgruppen berücksichtigen:

- Mehrere Datenbanken können nicht dieselbe ASM-Laufwerksgruppe (Automatic Storage Management) verwenden.
- Eine Laufwerksgruppe, die Datendateien enthält, kann keine anderen Dateitypen enthalten.
- Die LUN (Logical Unit Number) für die Datendatei-Festplattengruppe muss das einzige Objekt im Storage-Volume sein.

Nachfolgend sind einige Richtlinien für die Volume-Trennung aufgeführt:

- Die Datendateien für nur eine Datenbank müssen sich im Volume befinden.
- Sie müssen separate Volumes für jede der folgenden Dateiklassifizierungen verwenden: Datenbankbinärdateien, Datendateien, Online-Wiederherstellungsprotokolle, archivierte Wiederherstellungsprotokolle und Kontrolldateien.
- Sie müssen kein separates Volume für temporäre Datenbankdateien erstellen, da SnapManager keine temporären Datenbankdateien erstellt.

Definieren des Datenbank-Home mit der oratab-Datei

SnapManager verwendet die oratab-Datei während Operationen, um das Home-Verzeichnis der Oracle-Datenbank zu bestimmen. Ein Eintrag für Ihre Oracle-Datenbank muss in der oratab-Datei sein, damit SnapManager ordnungsgemäß funktionieren kann. Die oratab-Datei wird während der Oracle-Softwareinstallation erstellt.

Die oratab-Datei befindet sich an verschiedenen Orten, basierend auf dem Host-Betriebssystem, wie in der folgenden Tabelle dargestellt:

Host-Betriebssystem	Speicherort der Datei
Linux	/Etc/oratab
Solaris	/Var/opt/oracle/oratab
IBM AIX	/Etc/oratab

Die Beispiel-Oratab-Datei enthält die folgenden Informationen:

```
+ASM1:/u01/app/11.2.0/grid:N   # line added by Agent
oelpro:/u01/app/11.2.0/oracle:N         # line added by Agent
# SnapManager generated entry          (DO NOT REMOVE THIS LINE)
smoclone:/u01/app/11.2.0/oracle:N
```

Nach der Installation von Oracle müssen Sie sicherstellen, dass sich die oratab-Datei in dem in der vorherigen Tabelle angegebenen Speicherort befindet. Wenn sich die oratab-Datei nicht an dem richtigen Ort gemäß Ihrem Betriebssystem befindet, müssen Sie sich an den technischen Support wenden, um Hilfe zu erhalten.

Anforderungen für die Verwendung von RAC-Datenbanken mit SnapManager

Sie müssen die Empfehlungen für die Verwendung von RAC-Datenbanken (Real Application Clusters) mit SnapManager kennen. Die Empfehlungen umfassen Portnummern, Passwörter und den Authentifizierungsmodus.

- Im Datenbankauthentifizierungsmodus muss der Listener auf jedem Knoten, der mit einer Instanz der RAC-Datenbank interagiert, so konfiguriert werden, dass er dieselbe Portnummer verwendet.

  Der Listener, der mit der primären Datenbankinstanz interagiert, muss vor dem Start eines Backups

gestartet werden.

- Im Betriebssystem-Authentifizierungsmodus oder in einer ASM-Umgebung (Automatic Storage Management) muss der SnapManager-Server auf jedem Knoten der RAC-Umgebung installiert und ausgeführt werden.
- Das Benutzerpasswort für die Datenbank (z. B. für einen Systemadministrator oder einen Benutzer mit der sysdba-Berechtigung) muss für alle Oracle-Datenbankinstanzen in einer RAC-Umgebung identisch sein.

Anforderungen für die Verwendung von ASM-Datenbanken mit SnapManager

Sie müssen die Anforderungen für die Verwendung von ASM-Datenbanken (Automatic Storage Management) mit SnapManager kennen. Wenn Sie diese Anforderungen kennen, können Sie unter anderem Probleme mit den Spezifikationen ASMLib, Partitionen und Klonen vermeiden.

- SnapManager (3.0.3 oder höher) verwendet die neue sysasm-Berechtigung, die mit Oracle 11gR2 verfügbar ist, anstatt die sysdba-Berechtigung zur Verwaltung einer Oracle ASM-Instanz.

  Wenn Sie die sysdba-Berechtigung zum Ausführen von Administratorbefehlen auf der ASM-Instanz verwenden, wird eine Fehlermeldung angezeigt. Die Datenbank verwendet die sysdba-Berechtigung für den Zugriff auf Laufwerksgruppen. Wenn Sie eine Verbindung mit der ASM-Instanz über die sysasm-Berechtigung herstellen, haben Sie vollständigen Zugriff auf alle verfügbaren Oracle ASM-Festplattengruppen und Verwaltungsfunktionen.

  Wenn Sie Oracle 10gR2 und 11gR1 verwenden, müssen sie weiterhin die sysdba-Berechtigung verwenden.

- SnapManager (3.0.3 oder höher) unterstützt die Sicherung von Datenbanken, die direkt auf ASM-Festplattengruppen gespeichert sind, wenn die Laufwerksgruppe auch ein ACFS-Volume (Automatic Cluster File System) enthält.

  Diese Dateien sind indirekt durch SnapManager geschützt und werden möglicherweise mit dem restlichen Inhalt einer ASM-Festplattengruppe wiederhergestellt, aber SnapManager (3.0.3 oder höher) unterstützt kein ACFS.

  ACFS ist eine plattformübergreifende, skalierbare File-System-Storage-Management-Technologie, die mit Oracle 11gR2 verfügbar ist. ACFS erweitert die ASM-Funktionalität, um Kundendateien zu unterstützen, die außerhalb der Oracle-Datenbank gepflegt werden.

- SnapManager (3.0.3 oder höher) unterstützt die Sicherung von Dateien, die auf ASM-Festplattengruppen gespeichert sind, wenn die Laufwerksgruppe auch OCR-Dateien (Oracle Cluster Registry) oder Abstimmdiskdateien enthält. Wiederherstellungsvorgänge erfordern jedoch eine langsamere, hostbasierte oder PFSR-Methode (Partial File Snap Restore).

  Am besten sollten OCR- und Abstimmfestplatten auf Laufwerksgruppen vorhanden sein, die keine Datenbankdateien enthalten.

- Jedes für ASM verwendete Laufwerk darf nur eine Partition enthalten.
- Die Partition, die die ASM-Daten hostet, muss richtig ausgerichtet sein, um schwere Performanceprobleme zu vermeiden.

  Dies bedeutet, dass die LUN den korrekten Typ haben muss, und die Partition einen Offset mit einem

mehrere 4K Byte haben muss.

Weitere Informationen zum Erstellen von Partitionen, die auf 4K ausgerichtet sind, finden Sie im Knowledge Base-Artikel 1010717.

- ASM-Konfiguration ist nicht als Teil der Klonspezifikation angegeben.

  Sie müssen die ASM-Konfigurationsinformationen in den Klonspezifikationen, die mit SnapManager 2.1 erstellt wurden, manuell entfernen, bevor Sie den Host auf SnapManager (2.2 oder höher) aktualisieren.

- SnapManager 3.1, 3.1p1 und 3.2 oder höher unterstützen ASMLib 2.1.4.
- SnapManager 3.1p4 oder höher unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8.

Unterstützte Partitionsgeräte

Sie müssen die verschiedenen Partitionsgeräte kennen, die in SnapManager unterstützt werden.

Die folgende Tabelle enthält Partitionsinformationen und die Möglichkeit, diese für verschiedene Betriebssysteme zu aktivieren:

Betriebssystem	Einzelne Partition	Mehrere Partitionen	Geräte ohne Partitionierung	Dateisystem oder RAW-Geräte
Red hat Enterprise Linux 5x oder Oracle Enterprise Linux 5-mal	Ja.	Nein	Nein	Ext3*
Red hat Enterprise Linux 6 x oder Oracle Enterprise Linux 6x	Ja.	Nein	Nein	Ext3 oder ext4*
SUSE Linux Enterprise Server 11	Ja.	Nein	Nein	Ext3*
SUSE Linux Enterprise Server 10	Nein	Nein	Ja.	Erw. 3***
Red hat Enterprise Linux 5x oder Lateror Oracle Enterprise Linux 5-mal oder höher	Ja.	Nein	Ja.	ASM mit ASMlib**

Betriebssystem	Einzelne Partition	Mehrere Partitionen	Geräte ohne Partitionierung	Dateisystem oder RAW-Geräte
SUSE Linux Enterprise Server 10 SP4or SUSE Linux Enterprise Server 11	Ja.	Nein	Ja.	ASM mit ASMlib**
SUSE Linux Enterprise Server 10 SP4 oder Lateror SUSE Linux Enterprise Server 11	Ja.	Nein	Nein	ASM ohne ASMlib**

Weitere Informationen zu den unterstützten Betriebssystemversionen finden Sie in der Interoperabilitäts-Matrix.

Unterstützung für ASMLib

SnapManager unterstützt verschiedene Versionen von ASMLib, obwohl es mehrere Faktoren, die Sie bei der Verwendung von SnapManager mit ASMLib berücksichtigen müssen.

SnapManager unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8. Alle SnapManager-Vorgänge können mit ASMLib 2.1.4, 2.1.7 und 2.1.8 ausgeführt werden.

Wenn Sie von ASMLib 2.1.4 auf ASM 2.1.7 aktualisiert haben, können Sie die gleichen Profile und Backups verwenden, die mit ASMLib 2.1.4 erstellt wurden, um die Backups wiederherzustellen und die Klone zu erstellen.

Bei der Verwendung von SnapManager mit ASMLib müssen Sie Folgendes berücksichtigen:

- SnapManager 3.1 unterstützt ASMLib 2.1.7 nicht.

  SnapManager 3.1p4 oder höher unterstützt ASMLib 2.1.4, 2.1.7 und 2.1.8.

- Nach einem Rolling Upgrade von SnapManager 3.1 auf 3.2 funktionieren die mit ASMLib 2.1.7 erstellten Backups nur dann, wenn das Repository wieder auf SnapManager 3.1 und ASMLib 2.1.7 zurückgesetzt wird auf ASMLib 2.1.4.
- Nach einem Rolling Upgrade von SnapManager 3.1 auf 3.2 funktionieren Backups, die mit ASMLib 2.1.7 7 erstellt wurden, nicht, wenn das Repository mit ASMLib 2.1 zurück zu SnapManager 3.1 zurückgesetzt wird.

  Das Rollback ist erfolgreich, aber die Profile und Backups können nicht verwendet werden.

Unterstützung für ASM-Datenbanken ohne ASMLib

SnapManager unterstützt standardmäßig ASM ohne ASMLib. Die grundlegende Voraussetzung ist, dass die Geräte, die für ASM-Laufwerksgruppen verwendet werden,

partitioniert werden müssen.

Wenn ASMLib nicht installiert ist, werden die Geräteberechtigungen für ASM-Laufwerksgruppen in root:Disk geändert, wenn Sie die folgenden Vorgänge ausführen:

- Starten Sie den Host neu
- Wiederherstellen einer Datenbank aus dem primären Storage mithilfe von Volume-basierten SnapRestore (VBSR)
- Wiederherstellung einer Datenbank aus dem sekundären Storage

Sie können die entsprechenden Geräteberechtigungen festlegen, indem Sie der Konfigurationsoption oracleasm.Support.without.asmlib in smo.conf True zuweisen. Die mit den ASM-Laufwerksgruppen verbundenen Geräte werden beim Hinzufügen oder Entfernen neuer Geräte vom Host hinzugefügt oder aus der Datei initasmdisk entfernt. Die Datei initasmdics befindet sich unter /etc/initasmDisks.

Wenn Sie beispielsweise oracleasm.Support.without.asmlib=true festlegen und anschließend eine Sicherungshalterung durchführen, werden neue Geräte zu initasmDisks hinzugefügt. Beim Neustart des Hosts werden die Geräteberechtigungen und die Eigentumsrechte von den Startskripten beibehalten.

Der Standardwert für oracleasm.Support.without.asmlib ist false.

Verwandte Informationen

Unterstützte Partitionsgeräte

Unterstützte Skripte

Die Skripte asmmain.sh und asmquerydisk.sh ermöglichen das Ändern des Grid-Benutzers, der Gruppe und des Benutzers, die alle zur Abfrage der ASM-Laufwerke verwendet werden. Die Skripte müssen immer aus dem Root ausgeführt werden.

Die asmmain.sh ist die Skript-Hauptdatei, die von jedem Vorgang aufgerufen wird, der Geräte hinzufügt oder löscht. Das Skript asmmain.sh ruft intern ein anderes Skript auf, das vom Root ausgeführt werden muss, das über oracle Grid-Anmeldedaten verfügt. Dieses Skript fragt die Geräte der ASM-Laufwerksgruppe ab und fügt diese Einträge in der initasmdisk-Datei mit der Berechtigung und dem Eigentum der Geräte hinzu. Sie können die Berechtigungen und Eigentumsrechte dieser Datei basierend auf Ihrer Umgebung und dem regex-Muster ändern, das nur zur Übereinstimmung mit /dev/mapper/*p1 verwendet wird.

Das Skript asmquerydisk.sh wird verwendet, um die Festplattenliste abzufragen, die zur Erstellung der ASM-Laufwerksgruppe verwendet wird. Je nach Konfiguration müssen Sie Oracle_BASE, ORACLE_HOME und ORACLE_SID Werte zuweisen.

Die Skripte finden sich unter /opt/NetApp/smo/Plugins/examples/noasmlib. Diese Skripte müssen allerdings in die /opt/NetApp/smo/Plugins/noasmlib verschoben werden, bevor der SnapManager für Oracle Server auf dem Host gestartet wird.

Einschränkungen bei der Verwendung von Skripten zur Unterstützung einer ASM-Datenbank ohne ASMLib

Sie müssen sich über bestimmte Einschränkungen bei der Verwendung von Skripten zur Unterstützung einer ASM-Datenbank ohne ASMLib bewusst sein.

- Die Skripte stellen eine alternative Lösung für jede Kernel-Version dar, jedoch nur, wenn ASMLib nicht installiert ist.
- Die Berechtigungen für die Skripte müssen so festgelegt werden, dass Root-, Grid-, oracle- oder vergleichbare Benutzer auf die Skripte zugreifen können.
- Die Skripte unterstützen keine Wiederherstellung von einem sekundären Speicherort.

Implementieren und Ausführen der Skripte

Sie können die Skripte asmmain.sh und asmquerydisk.sh bereitstellen und ausführen, um ASM-Datenbanken ohne ASMLib zu unterstützen.

Diese Skripte folgen nicht der Pre-scripts oder Post-scripts Syntax und Workflow wird aufgerufen, wenn intitasmdisks aktiviert ist. Sie können in den Skripten alles ändern, was mit Ihren Konfigurationseinstellungen zusammenhängt. Es wird empfohlen zu überprüfen, ob alle Skripte mit einem kurzen Trockenlauf wie erwartet funktionieren.

Diese Skripte schaden Ihrem System weder bei Ausfällen noch werden sie Ihr System beeinträchtigen. Diese Skripte werden ausgeführt, um die ASM-bezogenen Laufwerke zu aktualisieren, um die richtigen Berechtigungen und Eigentumsrechte zu haben, so dass die Festplatten immer unter ASM-Instanz Kontrolle.

1. Erstellen Sie die ASM-Festplattengruppen mit den partitionierten Laufwerken.
2. Erstellen Sie die Oracle-Datenbank auf den FESTPLATTENGRUPPEN.
3. Beenden Sie den SnapManager für Oracle Server.

In einer RAC-Umgebung müssen Sie diesen Schritt auf allen RAC-Knoten durchführen.

4. Ändern Sie die smo.conf, um die folgenden Parameter einzuschließen:
   a. Oracleasm.Support.without.asmlib = true
   b. Oracleasm.Support.without.asmlib.Ownership = true
   c. oracleasm.support.without.asmlib.username = Benutzername Ihrer ASM-Instanzumgebung
   d. oracleasm.support.without.asmlib.groupname = Gruppenname Ihrer ASM-Instanzumgebung

   Durch diese Änderungen werden nur die Berechtigungen für den absoluten Pfad festgelegt, was bedeutet, dass anstelle des Partitionsgeräts die Berechtigungen nur für das dm-*-Gerät festgelegt werden.
5. Fügen Sie die Konfigurationseinstellungen in die Skripte der Plug-ins unter /opt/NetApp/smo/examples/noasmlib ein.
6. Kopieren Sie die Skripte in /opt/NetApp/smo/Plugins/noasmlib, bevor Sie den SnapManager für Oracle Server auf dem Host starten.
7. Navigieren Sie zum Verzeichnis /opt/NetApp/smo und führen Sie einen trockenen Lauf durch: sh Plug-ins/noasmlib/asmmain.sh

   Die etc/initasmdisks-Datei wird erstellt, was die Hauptdatei ist, die verwendet wird.

   Sie können bestätigen, dass die etc/initasmdisks-Datei alle Geräte enthält, die mit der konfigurierten ASM-Datenbank zusammenhängen, wie z. B.:

```
chown -R grid:oinstall /dev/mapper/360a98000316b61396c3f394645776863p1
         chmod 777 /dev/mapper/360a98000316b61396c3f394645776863p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714239p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714239p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714241p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714241p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714243p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714243p1
```

8. Starten Sie den SnapManager für Oracle-Server.
9. Konfigurieren Sie SnapDrive für UNIX, indem Sie die folgende Datei zur snapdrive.conf Datei hinzufügen.Disconnect-luns-before-vbsr=on
10. Starten Sie SnapDrive für UNIX Server neu.

> In einer RAC-Umgebung müssen Sie die Schritte 3 bis 10 für alle RAC-Knoten durchführen.

Die erstellte /etc/initasmdics-Datei muss entweder aus einem der Startskripte oder aus einem Skript ausgeführt werden, das in rc3.d. neu definiert ist Die Datei /etc/initasmdisks sollte immer ausgeführt werden, bevor der oracleha-Dienst gestartet wird.

Beispiel

```
# ls -ltr *ohasd*
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 S96ohasd ->
/etc/init.d/ohasd
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 K15ohasd ->
/etc/init.d/ohasd
```

Im folgenden Beispiel ist sh -x/etc/initasmdisks standardmäßig nicht verfügbar, und Sie müssen es als die erste Zeile der Funktion anhängen `start_stack()` In einem ohasd-Skript:

```
start_stack()
{
sh -x /etc/initasmdisks
# see init.ohasd.sbs for a full rationale case $PLATFORM in Linux
}
```

Unterstützung für Oracle RAC ASM-Datenbanken ohne ASMLib

Wenn Sie Oracle RAC-Datenbanken verwenden, müssen die RAC-Knoten mit der

Initasmdics-Datei aktualisiert werden, sobald ein Vorgang im Master RAC-Knoten ausgeführt wird.

Wenn sich vom Master-Knoten aus keine Authentifizierung bei den RAC-Knoten anmelden muss, führt der asmmain.sh eine sichere Kopie (SCP) von InitasmDisks an alle RAC-Knoten aus. Die InitasmDisks-Datei des Master-Knotens wird jedes Mal aufgerufen, wenn eine Wiederherstellung stattfindet. Das Skript asmmain.sh kann aktualisiert werden, um auf alle RAC-Knoten dasselbe Skript aufzurufen.

Die erstellte /etc/initasmdics-Datei, die entweder aus einem der Startskripte oder aus einem neu definierten Skript in rc3.d. ausgeführt werden muss Die Datei /etc/initasmdisks sollte immer ausgeführt werden, bevor der oracleha-Dienst gestartet wird.

Unterstützung für Oracle 10g ASM-Datenbanken ohne ASMLib

Wenn Sie Oracle 10g verwenden, steht der Befehl asmcmd nicht für die Auflistung von Disketten zur Verfügung. Sie können die sql-Abfrage verwenden, um die Festplattenliste abzurufen.

Das Script Disk_list.sql ist in die vorhandenen Skripte enthalten, die im Beispielverzeichnis zur Unterstützung von sql-Abfragen zur Verfügung gestellt werden. Wenn Sie theasmquerydisk.sh Skript ausführen, muss das Script Disk_list.sql manuell ausgeführt werden. Die Beispielzeilen werden mit Kommentaren in der Datei asmquerydisk.sh hinzugefügt. Diese Datei kann entweder am Speicherort /Home/Grid oder an einem anderen Ort Ihrer Wahl platziert werden.

Beispielskripts zur Unterstützung von ASM-Datenbanken ohne ASMLib

Die Beispielskripte sind im Verzeichnis Plugins/examples/noasmlib des Installationsverzeichnisses für SnapManager für Oracle verfügbar.

asmmain.sh

```
#!/bin/bash
griduser=grid
gridgroup=oinstall

# Run the script which takes the disklist from the asmcmd
# use appropriate user , here grid user is being used to run
# asmcmd command.
su -c "plugins/noasmlib/asmdiskquery.sh" -s /bin/sh grid
cat /home/grid/disklist

# Construct the final file as .bak file with propre inputs
awk -v guser=$griduser -v ggroup=$gridgroup '/^\/dev\/mapper/ { print
"chown -R "guser":"ggroup" "$1; print "chmod 777 " $1; }'
/home/grid/disklist > /etc/initasmdisks.bak

# move the bak file to the actual file.
mv /etc/initasmdisks.bak /etc/initasmdisks
```

```
# Set full full permission for this file to be called while rebooting and
restore
chmod 777 /etc/initasmdisks

# If the /etc/initasmdisks needs to be updated in all the RAC nodes
# or /etc/initasmdisks script has to be executed in the RAC nodes, then
the following
# section needs to be uncommented and used.
#
# Note: To do scp or running scripts in remote RAC node via ssh, it needs
password less login
# for root user with ssh keys shared between the two nodes.
#
# The following 2 lines are used for updating the file in the RAC nodes:
# scp /etc/initasmdisks root@racnode1:/etc/initasmdisks
# scp /etc/initasmdisks root@racnode2:/etc/initasmdisks
#
# In order to execute the /etc/initasmdisks in other RAC nodes
# The following must be added to the master RAC node /etc/initasmdisks
file
# from the asmmain.sh script itself. The above scp transfer will make sure
# the permissions and mode for the disk list contents are transferred to
the other RAC nodes
# so now appending any command in the /etc/initasmsdisks will be retained
only in the master RAC node.
# The following lines will add entries to the /etc/initasmsdisks file in
master RAC node only. When this script is executed
#  master RAC node, /etc/initasmdisks in all the RAC nodes will be
executed.
# echo 'ssh racnode1 /etc/initasmdisks' >> /etc/initasmdisks
# echo 'ssh racnode2 /etc/initasmdisks' >> /etc/initasmdisks
```

asmquerydisk.sh

```
#!/bin/bash
export  ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/grid/product/11.2.0.3/grid
export ORACLE_SID=+ASM
export  PATH=$ORACLE_HOME/bin:$PATH

# Get the Disk List and save this in a file called dglist.
asmcmd lsdsk  > /home/grid/disklist

# In oracle 10g the above used command 'asmcmd' is not available so use
SQL
# query can be used to take the disk list. Need to uncomment the following
# line and comment the above incase oracle 10g is being in use.
# The disk_list.sql script is availbe in this noasmlib examples folder
itself
# which can be modified as per customer needs.
# sqlplus "/as sysdba" @/home/grid/disk_list.sql > /home/grid/disklist
```

Disk_list.sql

```
# su - oracle
-bash-4.1$ cat disk_list.sql
select path from v$asm_disk;
exit
-bash-4.1$
```

Anforderungen für die Verwendung von Datenbanken mit NFS und SnapManager

Sie müssen die Anforderungen für die Verwendung von Datenbanken mit Network File System (NFS) und SnapManager kennen. Die Empfehlungen umfassen die Ausführung als root, Attribut-Caching und symbolische Links.

- Sie müssen SnapManager als Root ausführen. SnapManager muss auf die Dateisysteme zugreifen können, die Datendateien, Kontrolldateien, Online-Wiederherstellungsprotokolle, Archivprotokolle und den Datenbank-Home enthalten.

  Legen Sie eine der folgenden NFS-Exportoptionen fest, um sicherzustellen, dass Root auf die Dateisysteme zugreifen kann:

  - Root=Hostname
  - rw=Host-Name, anon=0
- Sie müssen das Attribut-Caching für alle Volumes deaktivieren, die Datenbankdatendateien, Kontrolldateien, Redo- und Archivprotokolle und die Datenbank-Startseite enthalten.

  Exportieren Sie die Volumes mithilfe der optionen noac (für Solaris und AIX) oder actimeo=0 (für Linux).

- Sie müssen die Datenbankdatendateien aus dem lokalen Speicher mit NFS verknüpfen, um nur symbolische Links auf Mount-Punkt-Ebene zu unterstützen.

Beispiel für Datenbank-Volume-Layouts

Weitere Informationen zur Konfiguration Ihrer Datenbank finden Sie unter Beispiel-Datenbank-Volume-Layouts.

Single-Instance-Datenbanken

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_sid	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_sid (Multiplexed) Oralogen02_sid (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Ja.	Aus

RAC-Datenbanken (Real Application Clusters)

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_dbname	Ja.	Aus
Temporäre Datendateien	Oratepp_dbname	Ja.	Aus
Kontrolldateien	Oracntrl01_dbname (Multiplexed) Oracntrl02_dbname (Multiplexed)	Ja.	Aus

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_dbname	Ja.	Aus
Cluster-Dateien	Oracrs_clustername	Ja.	Ein

Einzelne Instanz einer ASM-Datenbank (Automatic Storage Management

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Orabin_Host namelun	Ja.	Ein
Datendateien	Oradata_sid	Oradata_sidlun	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Oratepp_sidlun	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Oracntrl01_sidlun (Multiplexed) Oracntrl02_sidlun (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Oralog01_dbnamelun (Multiplexed) Oralogen02_dbnamelun (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Oraarch_sidlun	Ja.	Aus

ASM RAC-Datenbanken

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Orabin_Host namelun	Ja.	Ein

Dateitypen	Volume-Namen	LUN-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Datendateien	Oradata_sid	Oradata_sidlun	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Oratepp_sidlun	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Oracntrl01_sidlun (Multiplexed) Oracntrl02_sidlun (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_dbname (Multiplexed) Oralogen02_dbname (Multiplexed)	Oralog01_dbnamelun (Multiplexed) Oralogen02_dbnamelun (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Oraarch_sidlun	Ja.	Aus
Cluster-Dateien	Oracrs_clustername	Oracrs_clusternamelun	Ja.	Ein

Einschränkungen bei der Arbeit mit SnapManager

Sie müssen die Szenarien und Einschränkungen kennen, die sich auf Ihre Umgebung auswirken können.

Einschränkungen im Zusammenhang mit Datenbank-Layouts und Plattformen

- SnapManager unterstützt Steuerdateien auf einem Dateisystem in einer ASM-Laufwerksgruppe und unterstützt keine Steuerdateien auf RAW-Geräten.
- SnapManager arbeitet in einer Microsoft Clustering-Umgebung (MSCS), erkennt jedoch den Status der MSCS-Konfiguration (aktiv oder passiv) nicht und überträgt kein aktives Management eines Repositorys in einen Standby-Server in einem MSCS-Cluster.
- In Red hat Enterprise Linux (RHEL) und Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 und 5.3 wird das ext3-Dateisystem bei der Bereitstellung von Oracle über RAW-Geräte durch Verwendung von dynamischem Multipathing (DMP) in einer Multipath Network I/O (MPIO)-Umgebung nicht unterstützt.

  Dieses Problem ist in SnapManager nur bemerkt, wenn SnapDrive 4.1 für UNIX oder frühere Versionen verwendet wird.

- SnapManager unter RHEL unterstützt die Partitionierung von Festplatten mit dem Dienstprogramm **parted** nicht.

  Dies ist ein Problem mit dem Dienstprogramm RHEL **parted**.

- Wenn in einer RAC-Konfiguration ein Profilname aus RAC-Knoten A aktualisiert wird, wird die Zeitplandatei

für das Profil nur für RAC-Knoten A aktualisiert

Die Zeitplandatei für dasselbe Profil auf RAC-Knoten B wird nicht aktualisiert und enthält die früheren Terminplaninformationen. Wenn ein geplantes Backup von Knoten B ausgelöst wird, schlägt der geplante Backup-Vorgang fehl, da Node B die frühere Zeitplandatei enthält. Der geplante Sicherungsvorgang ist jedoch von Knoten A erfolgreich, auf dem das Profil umbenannt wird. Sie können den SnapManager-Server neu starten, sodass Sie die neueste Zeitplandatei für das Profil auf Knoten B. erhalten

- Die Repository-Datenbank kann auf einem Host vorhanden sein, auf den über mehrere IP-Adressen zugegriffen werden kann.

  Wenn über mehrere IP-Adressen auf das Repository zugegriffen wird, wird die Zeitplandatei für jede der IP-Adressen erstellt. Wenn die Backup-Planung für ein Profil (z. B. Profil A) unter einer der IP-Adressen (z. B. IP1) erstellt wird, wird die Zeitplandatei nur für diese IP-Adresse aktualisiert. Wenn von einer anderen IP-Adresse auf Profil A zugegriffen wird (z. B. IP2), wird das geplante Backup nicht aufgeführt, da die Terminplandatei von IP2 keinen Eintrag für den unter IP1 erstellten Zeitplan hat.

  Sie können warten, bis der Zeitplan von dieser IP-Adresse und der Zeitplandatei ausgelöst wird, oder Sie können den Server neu starten.

Einschränkungen in Bezug auf die SnapManager-Konfiguration

- SnapManager kann für die Katalogisierung von Datenbank-Backups mit RMAN konfiguriert werden.

  Wenn ein RMAN-Wiederherstellungskatalog verwendet wird, muss sich der Wiederherstellungskatalog in einer anderen Datenbank befinden als die gesicherte Datenbank.

- SnapDrive für UNIX unterstützt auf bestimmten Plattformen mehr als einen Filesystem- und Volume-Manager.

  Der für Datenbankdateien verwendete Dateisystem- und Volume-Manager muss in der SnapDrive-Konfigurationsdatei als Standarddateisystem und Volume Manager angegeben werden.

- SnapManager unterstützt Datenbanken auf MultiStore Storage-Systemen unter folgenden Anforderungen:
  - Sie müssen SnapDrive konfigurieren, um Passwörter für MultiStore Storage-Systeme festzulegen.
  - SnapDrive kann keine Snapshot Kopie einer LUN oder Datei in einem qtree in einem MultiStore Storage-System erstellen, wenn sich das zugrunde liegende Volume nicht im selben MultiStore Storage-System befindet.
- SnapManager unterstützt nicht den Zugriff auf zwei SnapManager Server, die auf verschiedenen Ports über einen einzelnen Client laufen (sowohl über CLI als auch über GUI).

  Die Port-Nummern sollten auf dem Ziel- und den Remote-Hosts identisch sein.

- Alle LUNs in einem Volume sollten auf Volume-Ebene oder in qtrees liegen, jedoch nicht beides.

  Das liegt daran, dass die Daten in den qtrees liegen und Sie das Volume mounten, dann sind die Daten in den qtrees nicht geschützt.

- SnapManager-Vorgänge schlagen fehl und Sie können nicht auf die GUI zugreifen, wenn die Repository-Datenbank ausfällt.

  Sie müssen überprüfen, ob die Repository-Datenbank ausgeführt wird, wenn Sie SnapManager-Vorgänge durchführen.

- SnapManager unterstützt keine Live Partition Mobility (LPM) und Live Application Mobility (LAM).
- SnapManager unterstützt Oracle Wallet Manager und Transparent Data Encryption (TDE) nicht.
- MetroCluster-Konfigurationen werden von SnapManager in RDM-Umgebungen (Raw Device Mapping) nicht unterstützt, da MetroCluster-Konfigurationen noch von der Virtual Storage Console (VSC) unterstützt werden müssen.

Einschränkungen im Zusammenhang mit der Profilverwaltung

- Wenn Sie das Profil aktualisieren, um die Backups des Archivprotokolls voneinander zu trennen, können Sie auf dem Host keinen Rollback-Vorgang durchführen.
- Wenn Sie ein Profil von der GUI aktivieren, um Archiv-Protokoll-Backups zu erstellen, und später versuchen, das Profil mithilfe des Fensters „Multi Profile Update“ oder des Fensters „Profile Update“ zu aktualisieren, können Sie dieses Profil nicht ändern, um ein vollständiges Backup zu erstellen.
- Wenn Sie im Fenster Multi Profile Update mehrere Profile aktualisieren und bei einigen Profilen die Option **Backup Archivilogs separat** aktiviert ist und andere Profile die Option deaktiviert haben, ist die Option **Archivprotokolle separat** sichern deaktiviert.
- Wenn Sie mehrere Profile aktualisieren und einige Profile die Option **Backup Archivilogs separat** aktivieren und andere Profile die Option deaktiviert haben, ist die Option **Backup Archivilogs separat** im Fenster Multi Profile Update deaktiviert.
- Wenn Sie das Profil umbenennen, können Sie den Host nicht zurückführen.

Einschränkungen im Zusammenhang mit Rolling Upgrade oder Rollback-Vorgängen

- Wenn Sie versuchen, eine frühere Version von SnapManager für einen Host zu installieren, ohne den Rollback-Vorgang auf dem Host im Repository durchzuführen, können Sie Folgendes möglicherweise nicht ausführen:
  - Sehen Sie sich die Profile an, die in früheren oder neueren Versionen von SnapManager für den Host erstellt wurden.
  - Greifen Sie auf Backups oder Klone zu, die in früheren oder neueren Versionen von SnapManager erstellt wurden.
  - Führen Sie Rolling Upgrade- oder Rollback-Vorgänge auf dem Host durch.
- Nachdem Sie die Profile getrennt haben, um Backups für Archivprotokolle zu erstellen, können Sie im zugehörigen Host Repository keinen Rollback-Vorgang durchführen.

Einschränkungen im Zusammenhang mit Backup-Vorgängen

- Die Backup-Erstellung kann fehlschlagen, wenn Sie SnapManager Vorgänge gleichzeitig auf demselben Host auf einer anderen ASM-Datenbank ausführen.
- Wenn der Backup während der Recovery bereits angehängt ist, mounted SnapManager den Backup nicht erneut und verwendet das bereits bereitgestellte Backup.

  Wenn das Backup von einem anderen Benutzer gemountet wird und Sie keinen Zugriff auf das zuvor bereitgestellte Backup haben, muss der andere Benutzer Ihnen die Berechtigung erteilen.

  Alle Archivprotokolldateien haben Leseberechtigung für Benutzer, die einer Gruppe zugewiesen sind. Sie haben möglicherweise nicht die Zugriffsberechtigung für die Archivprotokolldatei, wenn das Backup von einer anderen Benutzergruppe gemountet wird. Benutzer können die gemounteten Archivprotokolldateien manuell erteilen und den Wiederherstellungsvorgang oder die Wiederherstellung wiederholen.

- SnapManager legt den Backup-Status als „`PROTECTED`“ fest, selbst wenn eine der Snapshot-Kopien des

Datenbank-Backups auf das sekundäre Storage-System übertragen wird.

- Sie können die Aufgabenspezifikationsdatei nur für geplante Backups aus SnapManager 3.2 oder höher verwenden.
- Wenn ein Backup- oder Klonvorgang gleichzeitig auf den 10gR2- und 11gR2 RAC-Datenbanken über ASM ausgeführt wird, schlägt eine der Backup- oder Klonerstellung fehl.

  Dieser Fehler liegt an einer bekannten Oracle Einschränkung.

- SnapManager ist in den Protection Manager integriert und unterstützt das Backup mehrerer Volumes im Primärspeicher zu einem einzigen Volume im Sekundärspeicher von SnapVault und qtree SnapMirror.

  Die dynamische Dimensionierung eines sekundären Volumes wird nicht unterstützt. Weitere Informationen hierzu finden Sie im Provisioning Manager und Protection Manager – Administratorhandbuch für die Verwendung mit DataFabric Manager Server 3.8.

- SnapManager unterstützt mit dem Post-Processing-Skript nicht das Vaulting von Backups.
- Wenn die Repository-Datenbank auf mehr als eine IP-Adresse verweist und jede IP-Adresse einen anderen Hostnamen hat, ist der Backup-Planungsvorgang für eine IP-Adresse erfolgreich, schlägt aber für die andere IP-Adresse fehl.
- Nach einem Upgrade auf SnapManager 3.4 oder höher können alle mit Nachverarbeitungsskripten unter SnapManager 3.3.1 geplanten Backups nicht aktualisiert werden.

  Sie müssen den vorhandenen Zeitplan löschen und einen neuen Zeitplan erstellen.

Einschränkungen im Zusammenhang mit Wiederherstellungsvorgängen

- Wenn Sie eine indirekte Methode zur Durchführung eines Wiederherstellungsvorgangs verwenden und die für die Wiederherstellung erforderlichen Archivprotokolldateien nur bei Backups vom sekundären Speichersystem verfügbar sind, kann SnapManager die Datenbank nicht wiederherstellen.

  Der Grund dafür ist, dass SnapManager das Backup von Archivprotokolldateien nicht vom sekundären Storage-System mounten kann.

- Wenn SnapManager eine Volume-Wiederherstellung durchführt, werden die Backupkopien des Archivprotokolls, die nach der Wiederherstellung des entsprechenden Backups erstellt werden, nicht gelöscht.

  Wenn sich die Datendateien und das Ziel der Archivprotokolldatei auf demselben Volume befinden, können die Datendateien durch eine Wiederherstellung des Volumes wiederhergestellt werden, wenn im Ziel der Archivprotokolldatei keine Archivprotokolldateien vorhanden sind. In einem solchen Szenario gehen die Snapshot Kopien des Archivprotokolls verloren, die nach dem Backup der Dateien erstellt wurden.

  Sie sollten nicht alle Archivprotokolldateien vom Archivprotokollziel löschen.

- Wenn in einer ASM-Umgebung auf einer Laufwerksgruppe, die Datendateien hat, Oracle Cluster Registry (OCR) und Voting Disk-Dateien koexistieren, zeigt der Schnellwiederherstellungsvorgang die falsche Verzeichnisstruktur für den OCR- und Voting-Datenträger an.

Einschränkungen im Zusammenhang mit Klonvorgängen

- Aufgrund der Geschwindigkeit, mit der die Inodes vom Speichersystem erkannt und verarbeitet werden, das das flexible Volume enthält, können Sie keine numerischen Werte zwischen 0 und 100 für den Fortschritt des Clone-Split-Vorgangs anzeigen.

- SnapManager unterstützt nicht das Empfangen von E-Mails nur für erfolgreiche Klontrennvorgänge.
- SnapManager unterstützt nur die Aufteilung eines FlexClone.
- Das Klonen des Online-Datenbank-Backups der RAC-Datenbank, die den Speicherort der externen Archivprotokolldatei verwendet, ist aufgrund eines Fehlers bei der Wiederherstellung fehlgeschlagen.

  Das Klonen schlägt fehl, da Oracle die Archivprotokolldateien nicht für die Wiederherstellung vom externen Archivprotokollspeicherort findet und angewendet. Dies ist eine Einschränkung von Oracle. Weitere Informationen finden Sie unter Oracle Bug ID: 13528007. Oracle wendet Archivprotokoll nicht vom nicht standardmäßigen Speicherort auf dem an "Oracle Support Website". Sie müssen über einen gültigen Oracle metalink-Benutzernamen und ein gültiges Kennwort verfügen.

- SnapManager 3.3 oder höher unterstützt nicht mit der XML-Datei für die Klonspezifikation, die in den Versionen vor SnapManager 3.2 erstellt wurde.
- Wenn sich temporäre Tablespaces an einem anderen Speicherort als dem Datendateien befinden, erstellt ein Klonvorgang die Tabellen im Datendateien.

  Wenn jedoch temporäre Tablespaces Oracle Managed Files (OMFs) sind, die sich an einem anderen Speicherort als dem Datendateien befinden, erstellt der Klonvorgang nicht die Tabellen im Datendateien. Die OMFs werden nicht von SnapManager verwaltet.

- SnapManager kann eine RAC Datenbank nicht klonen, wenn Sie die Option -resetlogs auswählen.

Einschränkungen im Zusammenhang mit Archiv-Log-Dateien und Backups

- SnapManager unterstützt keine Anschnitt von Archiv-Log-Dateien aus dem Flash-Recovery-Bereich Ziel.
- SnapManager unterstützt nicht das Aufheben von Archivprotokolldateien vom Standby-Ziel.
- Die Backups für das Archivprotokoll werden basierend auf der Aufbewahrungsdauer und der standardmäßigen stündlichen Aufbewahrungsklasse beibehalten.

  Wenn die Klasse für die Backup-Aufbewahrung des Archivprotokolls über die SnapManager Befehlszeilenschnittstelle oder Benutzeroberfläche geändert wird, gilt die geänderte Aufbewahrungsklasse nicht für das Backup, da die Backups des Archivprotokolls basierend auf der Aufbewahrungsdauer aufbewahrt werden.

- Wenn Sie die Archivprotokolldateien aus den Zielen des Archivprotokolls löschen, enthält die Backup des Archivprotokolls keine Archivprotokolldateien, die älter sind als die fehlende Archivprotokolldatei.

  Wenn die letzte Archivprotokolldatei fehlt, schlägt die Sicherung des Archivprotokolls fehl.

- Wenn Sie die Archivprotokolldateien aus den Archivprotokollzielen löschen, schlägt das Beschneiden von Archivprotokolldateien fehl.
- SnapManager konsolidiert die Archiv-Log-Backups, selbst wenn Sie die Archiv-Log-Dateien aus den Archiv-Log-Zielen löschen oder wenn die Archiv-Log-Dateien beschädigt sind.

Einschränkungen im Zusammenhang mit der Änderung des Host-Namens der Zieldatenbank

Die folgenden SnapManager Vorgänge werden nicht unterstützt, wenn Sie den Host-Namen der Zieldatenbank ändern:

- Ändern des Host-Namens der Zieldatenbank von der SnapManager-GUI.
- Rollback der Repository-Datenbank nach Aktualisierung des Host-Namens der Zieldatenbank des Profils durchführen.

- Gleichzeitige Aktualisierung mehrerer Profile für einen neuen Hostnamen der Zieldatenbank.
- Ändern des Host-Namens der Zieldatenbank, wenn ein SnapManager-Vorgang ausgeführt wird.

Einschränkungen im Zusammenhang mit der SnapManager CLI oder GUI

- Die CLI-Befehle von SnapManager für den Vorgang zum Erstellen von Profilen, die über die Benutzeroberfläche von SnapManager generiert werden, verfügen über keine Optionen zur Verlaufskonfiguration.

  Mit dem Befehl „Profile create“ können Sie die Verlaufs-Aufbewahrungseinstellungen über die SnapManager-CLI konfigurieren.

- SnapManager zeigt die GUI in Mozilla Firefox nicht an, wenn auf dem UNIX-Client keine Java Runtime Environment (JRE) verfügbar ist.
- Wenn beim Aktualisieren des Host-Namens der Zieldatenbank mithilfe der SnapManager CLI eine oder mehrere offene SnapManager GUI-Sitzungen vorliegen, reagieren nicht alle offenen SnapManager GUI-Sitzungen.

Einschränkungen im Zusammenhang mit SnapMirror und SnapVault

- Das SnapVault Post-Processing-Skript wird nicht unterstützt, wenn Sie Data ONTAP 7-Mode verwenden.
- Wenn Sie ONTAP verwenden, können Sie Volume-basierte SnapRestore (VBSR) nicht auf den Backups ausführen, die in den Volumes erstellt wurden, über die SnapMirror Beziehungen festgelegt sind.

  Dies liegt an einer ONTAP Einschränkung, die es Ihnen nicht erlaubt, die Beziehung bei der Durchführung einer VBSR zu unterbrechen. Sie können jedoch eine VBSR beim letzten oder kürzlich erstellten Backup nur ausführen, wenn die Volumes SnapVault Beziehungen eingerichtet haben.

- Wenn Sie Data ONTAP in 7-Mode verwenden und eine VBSR für die Backups ausführen möchten, die in den Volumes erstellt wurden, auf denen SnapMirror Beziehungen festgelegt sind, können Sie die Option override-vbsr-snapmirror-Check in SnapDrive für UNIX auf ON setzen.

  Weitere Informationen dazu finden Sie in der SnapDrive-Dokumentation.

- In einigen Szenarien können Sie das letzte Backup, das mit der ersten Snapshot Kopie verbunden ist, nicht löschen, wenn das Volume eine SnapVault-Beziehung eingerichtet hat.

  Sie können das Backup nur löschen, wenn Sie die Beziehung unterbrechen. Dieses Problem liegt an einer ONTAP-Einschränkung bei Basis-Snapshot-Kopien. In einer SnapMirror Beziehung wird die Snapshot Basiskopie von der SnapMirror Engine erstellt und in einer SnapVault Beziehung ist die Snapshot Basiskopie das Backup, das mit SnapManager erstellt wurde. Die Basis-Snapshot-Kopie verweist bei jedem Update auf das neueste Backup, das mithilfe von SnapManager erstellt wird.

Einschränkungen im Zusammenhang mit Data Guard Standby-Datenbanken

- SnapManager unterstützt keine Standby-Datenbanken für die logische Datenwache.
- SnapManager unterstützt keine Standby-Datenbanken für Active Data Guard.
- SnapManager erlaubt keine Online-Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine partiellen Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt nicht die Wiederherstellung von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine Beschneidung von Archivprotokolldateien für Data Guard Standby-

Datenbanken.

- SnapManager unterstützt den Broker nicht.

Verwandte Informationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

SnapManager Limitierungen für Clustered Data ONTAP

Sie müssen die Einschränkungen für einige Funktionalitäten und SnapManager-Vorgänge kennen, wenn Sie Clustered Data ONTAP verwenden.

Die folgenden Funktionalitäten werden nicht unterstützt, wenn Sie SnapManager auf Clustered Data ONTAP nutzen:

- Datensicherungsfunktionen, wenn SnapManager in OnCommand Unified Manager integriert ist
- Eine Datenbank, in der eine LUN zu einem System gehört, auf dem Data ONTAP 7-Mode und die andere LUN ausgeführt werden, gehört zu einem System mit Clustered Data ONTAP
- SnapManager für Oracle unterstützt keine Migration von Vserver, wie sie von Clustered Data ONTAP nicht unterstützt wird
- SnapManager für Oracle unterstützt die Funktion Clustered Data ONTAP 8.2.1 nicht zur Festlegung verschiedener Exportrichtlinien für Volumes und qtrees

Einschränkungen in Bezug auf Oracle Database

Bevor Sie mit der Arbeit mit SnapManager beginnen, müssen Sie die Einschränkungen in Bezug auf Oracle Database kennen.

Die Einschränkungen sind wie folgt:

- SnapManager unterstützt Oracle Versionen 10gR2, 11gR1, 11gR2 und 12*c*, unterstützt aber Oracle 10gR1 als Repository oder Zieldatenbank nicht.
- SnapManager unterstützt die Verwendung einer SCAN-IP-Adresse anstelle eines Hostnamens nicht.

  SCAN-IP ist eine neue Funktion in Oracle 11gR2.

- Oracle Cluster File System (OCFS) wird von SnapManager nicht unterstützt.
- Oracle 11g in einer Direct NFS-Umgebung (dNFS) ermöglicht zusätzliche Mount-Point-Konfigurationen in der oranfstab-Datei, z. B. mehrere Pfade für den Lastausgleich.

  SnapManager ändert die oranfstab-Datei nicht. Sie müssen in der oranfstab-Datei manuell weitere Eigenschaften hinzufügen, die die geklonte Datenbank verwenden soll.

- Unterstützung für Oracle Database 9i ist veraltet aus SnapManager 3.2.
- Der Support für Oracle Database 10gR2 (früher als 10.2.0.5) ist veraltet aus SnapManager 3.3.1.

Ermitteln Sie die verschiedenen Versionen von Oracle Datenbanken, die durch die Interoperabilitäts-Matrix unterstützt werden.

Verwandte Informationen

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Veraltete Versionen der Oracle-Datenbank

Oracle Database 9i wird von SnapManager 3.2 oder höher nicht unterstützt, und die Oracle Database 10gR2 (früher als 10.2.0.4) wird von SnapManager 3.3.1 oder höher nicht unterstützt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und auf SnapManager 3.2 oder höher aktualisieren möchten, können Sie keine neuen Profile erstellen. Eine Warnmeldung wird angezeigt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und ein Upgrade auf SnapManager 3.2 oder höher durchführen möchten, müssen Sie eine der folgenden Aktionen durchführen:

- Aktualisieren Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken auf entweder Oracle 10gR2 (10.2.0.5), 11gR1 oder 11gR2 Datenbanken und führen Sie ein Upgrade auf SnapManager 3.2 oder 3.3 durch.

  Wenn Sie ein Upgrade auf Oracle 12*c* durchführen, müssen Sie ein Upgrade auf SnapManager 3.3.1 oder höher durchführen.

  Oracle Datenbank 12*c* wird nur von SnapManager 3.3 unterstützt.

- Verwalten Sie die Oracle 9i-Datenbanken mit einer Patch-Version von SnapManager 3.1.

  Sie können SnapManager 3.2 oder 3.3 verwenden, wenn Sie Oracle 10gR2-, 11gR1- oder 11gR2-Datenbanken verwalten und SnapManager 3.3.1 oder höher verwenden möchten, wenn Sie Oracle 12*c* -Datenbanken zusammen mit anderen unterstützten Datenbanken verwalten möchten.

Einschränkungen beim Volume-Management

Bei SnapManager gibt es bestimmte Volume-Management-Einschränkungen, die sich auf Ihre Umgebung auswirken können.

Sie können mehrere Laufwerksgruppen für eine Datenbank haben. Die folgenden Einschränkungen gelten jedoch für alle Festplattengruppen für eine bestimmte Datenbank:

- Plattengruppen für die Datenbank können nur von einem Volume-Manager verwaltet werden.
- Von einem logischen Volume-Manager gesicherte RAW-Geräte werden für den Schutz von Oracle Daten nicht unterstützt.

  RAW Device Storage und Automatic Storage Management (ASM)-Festplattengruppen müssen direkt auf physischen Geräten bereitgestellt werden. In einigen Fällen ist eine Partitionierung erforderlich.

- Eine Linux-Umgebung ohne logisches Volume-Management erfordert eine Partition.

Upgrade von SnapManager

Sie können von einer der früheren Versionen auf die neueste Version von SnapManager für Oracle aktualisieren. Sie können entweder alle SnapManager Hosts gleichzeitig aktualisieren oder ein Rolling Upgrade durchführen, wodurch Sie die Hosts auf

gestaffelte, Host-für-Host-Art aktualisieren können.

SnapManager wird vorbereitet

Die Umgebung, in der Sie ein SnapManager-Upgrade durchführen möchten, muss die spezifischen Software-, Hardware-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Aktuelle Informationen zu den Anforderungen finden Sie in der Interoperabilitäts-Matrix.

Sie müssen vor dem Upgrade sicherstellen, dass Sie die folgenden Aufgaben ausführen:

- Führen Sie die erforderlichen Vorinstallationsaufgaben aus.
- Laden Sie das neueste Installationspaket von SnapManager für Oracle herunter.
- Installieren und konfigurieren Sie die entsprechende Version von SnapDrive für UNIX auf allen Ziel-Hosts.
- Erstellen eines Backups der vorhandenen Repository-Datenbank SnapManager für Oracle

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Aktualisieren der SnapManager-Hosts

Sie können alle vorhandenen Hosts auf die neueste Version von SnapManager aktualisieren. Alle Hosts werden gleichzeitig aktualisiert. Dies kann jedoch zu einer Ausfallzeit aller SnapManager-Hosts und der geplanten Operationen während dieser Zeit führen.

1. Melden Sie sich beim Hostsystem als Root-Benutzer an.
2. Navigieren Sie von der Befehlszeilenschnittstelle (CLI) zu dem Speicherort, an dem Sie die Installationsdatei heruntergeladen haben.
3. Wenn die Datei nicht ausführbar ist, ändern Sie die Berechtigungen: `chmod 544 netapp.smo*`
4. Stoppen Sie den SnapManager Server: `smo_server stop`
5. Je nach UNIX Host, installieren Sie SnapManager:

Wenn das Betriebssystem…	Starten Sie dann…
Solaris (SPARC64)	
Solaris (x86_64)	
AIX (PPC64)	
• Linux x86*	
• Linux x64*	

6. Drücken Sie auf der Einführungsseite **Enter**, um fortzufahren.

Die folgende Meldung wird angezeigt: Vorhandene SnapManager für Oracle erkannt.

7. Drücken Sie **Enter**.
8. Führen Sie an der Eingabeaufforderung Folgendes aus:

   a. Drücken Sie **Enter**, um den Standardwert für den Benutzer des Betriebssystems zu übernehmen.
   b. Geben Sie den richtigen Wert für die Betriebssystemgruppe ein, oder drücken Sie **Enter**, um den Standardwert zu akzeptieren.
   c. Geben Sie den richtigen Wert für den Starttyp des Servers ein, oder drücken Sie **Enter**, um den Standardwert zu akzeptieren.

   Die Konfigurationsübersicht wird angezeigt.

9. Drücken Sie **Enter**, um fortzufahren.

   Die folgende Meldung wird angezeigt: Die Deinstallation von vorhandenem SnapManager für Oracle hat begonnen.

   Die Deinstallation ist abgeschlossen und die aktuelle Version von SnapManager ist installiert.

Aufgaben nach dem Upgrade

Nach dem Upgrade auf eine neuere Version von SnapManager müssen Sie das vorhandene Repository aktualisieren. Möglicherweise möchten Sie auch die Backup-Aufbewahrungsklasse, die dem bestehenden Backup zugewiesen ist, ändern. Ermitteln Sie dann, welchen Restore-Prozess Sie verwenden können.

Nach dem Upgrade auf SnapManager 3.3 oder höher müssen Sie sqlnet.authentication_services auf NONE setzen, wenn Sie die Datenbank-Authentifizierung (DB) als einzige Authentifizierungsmethode verwenden möchten. Diese Funktion wird für RAC-Datenbanken nicht unterstützt.

Das vorhandene Repository wird aktualisiert

Sie müssen das vorhandene Repository nicht aktualisieren, wenn Sie ein Upgrade von SnapManager 3.3.x auf SnapManager 3.4 oder höher durchführen. Für alle anderen Upgrade-Pfade müssen Sie jedoch das vorhandene Repository aktualisieren, damit Sie nach dem Upgrade darauf zugreifen können.

- Der aktualisierte SnapManager-Server muss gestartet und verifiziert worden sein.
- Ein Backup des vorhandenen Repositorys muss vorhanden sein.
- Wenn Sie ein Upgrade von einer älteren Version als SnapManager 3.1 auf SnapManager 3.3 oder höher durchführen, müssen Sie zuerst auf SnapManager 3.2 aktualisieren.

  Nach dem Upgrade auf SnapManager 3.2 können Sie dann ein Upgrade auf SnapManager 3.3 oder höher durchführen.

- Nach dem Aktualisieren des Repositorys können Sie das Repository nicht mit einer früheren SnapManager-Version verwenden.

a. Aktualisieren des vorhandenen Repositorys: `smo repository update -repository -dbname repository_service_name -host repository_host_name -login -username repository_user_name -port repository_port`

- Der Repository-Benutzername, der Repository-Dienstname und der Repository-Hostname können aus alphanumerischen Zeichen, einem Minuszeichen, einem Unterstrich und einem Zeitraum bestehen.
- Der Repository-Port kann eine beliebige gültige Portnummer sein. Die anderen Optionen, die beim Aktualisieren des vorhandenen Repositorys verwendet werden, sind wie folgt:
- Die Option Kraft
- Die Option noprompt
- Die ruhige Option
- Die ausführliche Option

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521

+
```

Starten Sie den SnapManager-Server neu, um die zugehörigen Zeitpläne neu zu starten.

Ändern der Backup-Aufbewahrungsklasse

Nach dem Upgrade weist SnapManager den vorhandenen Backups die standardmäßige Backup-Aufbewahrungsklasse zu. Sie können die Standardwerte für die Aufbewahrungsklassen entsprechend Ihren Backup-Anforderungen ändern.

Die standardmäßige Backup-Aufbewahrungsklasse, die den vorhandenen Backups zugewiesen ist, lautet wie folgt:

Backup-Typ	Zuweisung von Aufbewahrungsklassen nach Upgrade
Backups werden für immer aufbewahrt	Unbegrenzt
Andere Backups	Täglich

Hinweis: Sie können die Backups löschen, die für immer aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Wenn Sie ein Upgrade auf SnapManager 3.0 oder höher durchführen, werden den vorhandenen Profilen der größere der folgenden beiden Werte zugewiesen:

- Vorherige Aufbewahrungsanzahl für das Profil
- Standardwerte für die Aufbewahrungsanzahl und die Dauer der täglichen Backups, wie in der smo.config Datei angegeben

a. Ändern Sie die Werte, die in der Datei smo.config der Datei contac.hourly.count zugewiesen wurden,

und behalten Sie.hourly.duration bei.

Sie können die folgenden Werte eingeben:

- Beibehalten.hourly.count = 12
- Beibehalten.hourly.duration = 2

Verwandte Informationen

SnapManager-Konfigurationsparameter

Prozessarten wiederherstellen

Alle Restore-Prozesse werden nicht in allen SnapManager für Oracle Versionen unterstützt. Nach dem Upgrade von SnapManager müssen Sie auf den Wiederherstellungsprozess achten, den Sie zum Wiederherstellen eines Backups verwenden können.

Die mit SnapManager 3.0 oder höher erstellten Backups können sowohl mit schnellen Restore- als auch mit dateibasierten Restore-Prozessen wiederhergestellt werden. Die Backups, die mit einer älteren Version als SnapManager 3.0 erstellt wurden, können jedoch nur mit dem dateibasierten Wiederherstellungsprozess wiederhergestellt werden.

Sie können die zum Erstellen des Backups verwendete SnapManager-Version bestimmen, indem Sie den Befehl -Backup show ausführen.

Verwandte Informationen

Was ist Datenbank-Restore

Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade

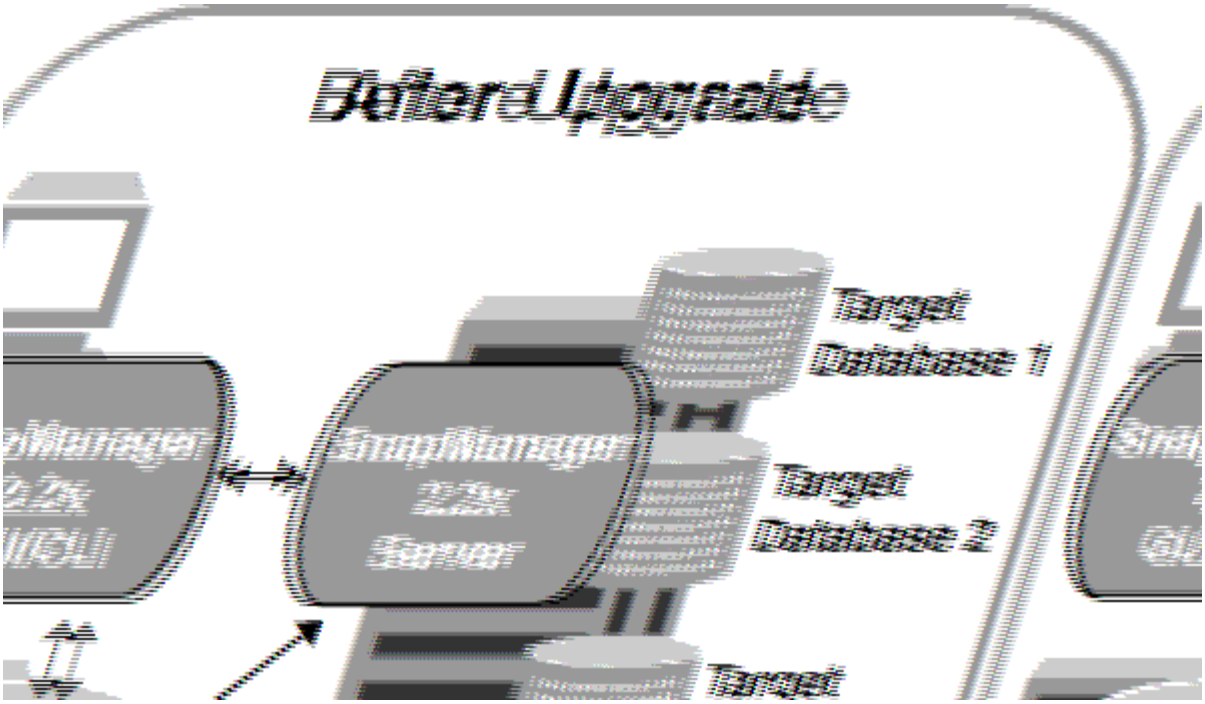
Der Rolling Upgrade-Ansatz, mit dem Sie Hosts auf gestaffelte, Host-für-Host-Art aktualisieren können, wird von SnapManager 3.1 unterstützt.

Mit SnapManager 3.0 oder einer älteren Version konnten Sie nur alle Hosts gleichzeitig aktualisieren. Dies führte zu Ausfallzeiten aller SnapManager-Hosts und der geplanten Betrieb während des Upgrade-Vorgangs.

Das Rolling Upgrade bietet folgende Vorteile:

- Verbesserte SnapManager Performance, da nur ein Host gleichzeitig aktualisiert wird.
- Fähigkeit, die neuen Funktionen auf einem SnapManager Server Host zu testen, bevor ein Upgrade der anderen Hosts durchgeführt wird

Rolling Upgrades können nur über die Befehlszeilenschnittstelle (CLI) durchgeführt werden.



Nach erfolgreichem Abschluss des Rolling Upgrade verfügen die SnapManager Hosts, Profile, Zeitpläne, Backups, Klone, die mit den Profilen der Zieldatenbanken verbunden sind, werden von der Repository-Datenbank der früheren SnapManager Version in die Repository-Datenbank der neuen Version migriert. Details zu den Vorgängen, die mithilfe der Profile, Zeitpläne, Backups und Klone, die in der früheren SnapManager Version erstellt wurden, stehen nun in der Repository-Datenbank der neuen Version zur Verfügung. Sie können die GUI mit den Standardkonfigurationswerten der Datei user.config starten. Die in der Datei User.config der früheren Version von SnapManager konfigurierten Werte werden nicht berücksichtigt.

Der aktualisierte SnapManager-Server kann jetzt mit der aktualisierten Repository-Datenbank kommunizieren. Die Hosts, die kein Upgrade durchgeführt haben, können ihre Zieldatenbanken mithilfe des Repositorys der früheren Version von SnapManager managen. Somit können die in der früheren Version verfügbaren Funktionen genutzt werden.

Bevor Sie ein Rolling Upgrade durchführen, müssen Sie sicherstellen, dass alle Hosts unter der Repository-Datenbank aufgelöst werden können. Informationen zur Lösung der Hosts finden Sie im Abschnitt zur Fehlerbehebung in *SnapManager for Oracle Administration Guide for UNIX*.

Verwandte Informationen

Was ist ein Rollback

SnapManager zur Fehlerbehebung

Voraussetzungen für Rolling Upgrades

Bevor Sie ein Rolling Upgrade durchführen, müssen Sie sicherstellen, dass Ihre Umgebung bestimmte Anforderungen erfüllt.

- Wenn Sie eine ältere Version als SnapManager 3.1 verwenden und ein Rolling Upgrade auf SnapManager 3.3 oder höher durchführen möchten, müssen Sie zuerst auf 3.2 und dann auf die neueste Version aktualisieren.

  Sie können direkt von SnapManager 3.2 auf SnapManager 3.3 oder höher aktualisieren.

- Externe Skripte, die zur Durchführung externer Datensicherung oder Datenaufbewahrung verwendet werden, müssen gesichert werden.
- Die SnapManager-Version, auf die Sie aktualisieren möchten, muss installiert sein.

> Wenn Sie ein Upgrade von einer älteren Version als SnapManager 3.1 auf SnapManager 3.3 oder höher durchführen, müssen Sie zuerst SnapManager 3.2 installieren und ein Rolling Upgrade durchführen. Nach dem Upgrade auf 3.2 können Sie SnapManager 3.3 oder höher installieren und ein weiteres Rolling Upgrade auf SnapManager 3.3 oder höher durchführen.

- Die SnapDrive für UNIX-Version, die von der SnapManager-Version unterstützt wird, auf die Sie aktualisieren möchten, muss installiert sein.

  Die SnapDrive-Dokumentation enthält Details zur Installation von SnapDrive.

- Die Repository-Datenbank muss gesichert werden.
- Die SnapManager Repository-Auslastung sollte mindestens betragen.
- Wenn der zu aktualisierenden Host ein Repository verwendet, dürfen SnapManager-Vorgänge nicht auf den anderen Hosts ausgeführt werden, die dasselbe Repository verwenden.

  Die Vorgänge, die auf den anderen Hosts geplant oder ausgeführt werden, warten bis das Rolling Upgrade abgeschlossen ist.

> Es wird empfohlen, ein Rolling Upgrade durchzuführen, wenn das Repository am wenigsten ausgelastet ist, z. B. über das Wochenende oder wenn Vorgänge nicht geplant sind.

- Profile, die auf dieselbe Repository-Datenbank verweisen, müssen mit unterschiedlichen Namen in den SnapManager-Server-Hosts erstellt werden.

  Wenn Sie Profile mit dem gleichen Namen verwenden, schlägt das Rolling Upgrade der Repository-Datenbank ohne Warnung fehl.

- SnapManager-Vorgänge dürfen nicht auf dem Host ausgeführt werden, der gerade aktualisiert wird.

> Das Rolling Upgrade wird länger ausgeführt, wenn die Anzahl der Backups der Hosts, die zusammen aktualisiert werden, steigt. Die Dauer des Upgrades kann je nach Anzahl der Profile und Backups variieren, die mit einem bestimmten Host verbunden sind.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Durchführung von Rolling Upgrade auf einem einzelnen oder mehreren Hosts

Sie können Rolling Upgrades für einen einzelnen oder mehrere SnapManager Server Hosts über die Befehlszeilenschnittstelle (CLI) durchführen. Der aktualisierte SnapManager-Server-Host wird dann nur mit der späteren Version von SnapManager verwaltet.

Sie müssen sicherstellen, dass alle Voraussetzungen für das Durchführen eines Rolling Upgrades abgeschlossen sind.

1. Um ein Rolling Upgrade auf einem einzelnen Host durchzuführen, geben Sie den folgenden Befehl ein:

'smorelepory RollingUpgrade-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-Upgradehosthost_with_target_Database-Force [-quiet [-verbose]'

Der folgende Befehl führt das Rolling Upgrade aller auf HostA eingebundenen Zieldatenbanken und einer Repository-Datenbank namens repoA auf repo_Host durch:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -upgradehost hostA
```

2. Um ein Rolling Upgrade auf mehreren Hosts durchzuführen, geben Sie den folgenden Befehl ein: 'smoreporory RollingUpgrade-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-Upgradehosthost_with_Target_database1,Host_with_Target_database2-Force [-quiet/ -verbose]'

   Geben Sie bei mehreren Hosts die durch Komma getrennten Hostnamen ein, und stellen Sie sicher, dass Sie keinen Speicherplatz zwischen dem Komma und dem nächsten Hostnamen angeben.Wenn Sie eine RAC-Konfiguration (Real Application Clusters) verwenden, müssen Sie alle RAC-verbundenen Hosts manuell aktualisieren. Sie können -allhosts verwenden, um das Rolling Upgrade aller Hosts durchzuführen.

   Der folgende Befehl führt das Rolling Upgrade aller auf den Hosts eingebundenen Zieldatenbanken, hostA und hostB sowie einer Repository-Datenbank namens repoA auf repo_Host durch:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -upgradehost hostA,hostB
```

3. Um ein Rolling Upgrade auf allen Hosts einer Repository-Datenbank durchzuführen, geben Sie den folgenden Befehl ein: 'smorepository rollingUpgrade-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-allhosts-Force [-quiet - verbose]'

   Nachdem Sie die Repository-Datenbank erfolgreich aktualisiert haben, können Sie alle SnapManager-Vorgänge auf der Zieldatenbank ausführen.

   Beim aktualisierten SnapManager für Oracle bleiben die hostbasierten Benutzeranmeldeinformationen, die Anmeldedaten für Oracle Software-Benutzer und die Anmeldedaten für den Oracle Recovery Manager (RMAN) von der früheren Version von SnapManager für Oracle erhalten.

Der folgende Befehl führt das Rolling Upgrade aller Zieldatenbanken durch, die in einer Repository-Datenbank mit dem Namen „repoA“ auf repo_Host verfügbar sind:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
      -allhosts
```

- Wenn der SnapManager-Server automatisch startet, müssen Sie den Server neu starten, um sicherzustellen, dass Sie die Zeitpläne anzeigen können.
- Wenn Sie einen der beiden zugehörigen Hosts aktualisieren, müssen Sie nach dem ersten Upgrade des zweiten Hosts ein Upgrade durchführen.

  Wenn Sie beispielsweise einen Klon von Host A nach Host B erstellt oder ein Backup von Host A an Host B angehängt haben, hängen die Hosts A und B miteinander zusammen. Wenn Sie Host A aktualisieren, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, den Host B bald nach dem Upgrade von Host A zu aktualisieren

> Die Warnmeldungen werden angezeigt, obwohl der Klon gelöscht wurde oder das Backup während des Rolling Upgrades von Host A von Host B abgehängt wurde Dies liegt daran, dass Metadaten im Repository für die Vorgänge vorhanden sind, die auf dem Remote-Host durchgeführt werden.

Verwandte Informationen

Voraussetzungen für Rolling Upgrades

Was ist ein Rollback

Mit dem Rollback-Vorgang können Sie nach einem Rolling Upgrade auf eine frühere SnapManager-Version zurücksetzen.

> Bevor Sie ein Rollback durchführen können, müssen Sie sicherstellen, dass alle Hosts unter der Repository-Datenbank aufgelöst werden können.

Wenn Sie ein Rollback durchführen, werden die folgenden Schritte zurückgesetzt:

- Backups, die erstellt, freigegeben und gelöscht wurden, verwenden Sie dazu die SnapManager Version, von der Sie ein Rollback durchführen
- Klone, die anhand eines Backups erstellt wurden, die mit der SnapManager Version erstellt wurden, von der aus Sie ein Rollback durchführen
- Profildaten wurden mithilfe der SnapManager-Version geändert, von der aus Sie ein Rollback ausführen
- Sicherungsstatus des Backups, das mit der SnapManager-Version geändert wurde, von der aus Sie ein Rollback durchführen

Die Funktionen, die in der von Ihnen verwendeten SnapManager-Version verfügbar waren, aber in der Version, auf die Sie zurückrollt, nicht verfügbar sind, werden nicht unterstützt. Wenn Sie beispielsweise ein Rollback von SnapManager 3.3 oder neuer zu SnapManager 3.1 durchführen, wird die Verlaufskonfiguration für Profile in SnapManager 3.3 oder höher nicht auf die Profile in SnapManager 3.1 zurückgesetzt. Dies liegt daran, dass die Verlaufskonfiguration in SnapManager 3.1 nicht verfügbar war.

Verwandte Informationen

SnapManager zur Fehlerbehebung

Einschränkungen bei der Durchführung eines Rollbacks

Sie müssen die Szenarien kennen, in denen Sie kein Rollback durchführen können. In einigen dieser Szenarien können Sie jedoch einige zusätzliche Aufgaben ausführen, bevor Sie das Rollback durchführen.

Die Szenarien, in denen Sie kein Rollback durchführen können oder die zusätzlichen Aufgaben ausführen müssen, sind wie folgt:

- Wenn Sie nach einem Rolling Upgrade einen der folgenden Vorgänge ausführen:
  - Erstellen Sie ein neues Profil.
  - Teilen Sie einen Klon auf.
  - Ändern Sie den Schutzstatus des Profils.
  - Zuweisung von Sicherungsrichtlinien, Aufbewahrungsklassen oder SnapVault- und SnapMirror-Beziehungen

    In diesem Szenario müssen Sie nach dem Durchführen eines Rollback die zugewiesene Sicherungsrichtlinie, die Aufbewahrungsklasse oder die zugewiesene SnapVault- und SnapMirror-Beziehung manuell entfernen.

  - Ändern Sie den Mount-Status des Backups.

    In diesem Szenario müssen Sie zuerst den Mount-Status in den ursprünglichen Zustand ändern und dann ein Rollback durchführen.

  - Stellen Sie ein Backup wieder her.
  - Ändern Sie den Authentifizierungsmodus von der Datenbankauthentifizierung in die Betriebssystemauthentifizierung.

    In diesem Szenario müssen Sie nach einem Rollback den Authentifizierungsmodus manuell von OS in die Datenbank ändern.
- Wenn der Hostname des Profils geändert wird
- Wenn Profile getrennt sind, um Archiv-Log-Backups zu erstellen

  In diesem Szenario können Sie keine Rollbacks auf eine Version durchführen, die früher als SnapManager 3.2 ist.

Voraussetzungen für die Durchführung eines Rollbacks

Bevor Sie ein Rollback durchführen, müssen Sie sicherstellen, dass Ihre Umgebung

bestimmte Anforderungen erfüllt.

- Wenn Sie SnapManager 3.3 oder höher verwenden und zu einer älteren Version als SnapManager 3.1 zurückkehren möchten, müssen Sie ein Rollback auf 3.2 und dann auf die gewünschte Version durchführen.
- Externe Skripte, die zur Durchführung externer Datensicherung oder Datenaufbewahrung verwendet werden, müssen gesichert werden.
- Die SnapManager-Version, auf die Sie einen Rollback ausführen möchten, muss installiert sein.

> Wenn Sie ein Rollback von SnapManager 3.3 oder neuer auf eine Version vor SnapManager 3.1 durchführen möchten, müssen Sie zuerst SnapManager 3.2 installieren und ein Rollback durchführen. Nach einem Rollback auf 3.2 können Sie SnapManager 3.1 oder eine frühere Version installieren und ein weiteres Rollback auf diese Version durchführen.

- Die SnapDrive für UNIX-Version, die mit der SnapManager-Version unterstützt wird, zu der Sie einen Rollback ausführen möchten, muss installiert sein.

  Informationen zum Installieren von SnapDrive finden Sie unter SnapDrive-Dokumentationssatz.

- Die Repository-Datenbank muss gesichert werden.
- Wenn der zurückzugerollte Host ein Repository verwendet, dürfen SnapManager-Vorgänge nicht auf den anderen Hosts ausgeführt werden, die dasselbe Repository verwenden.

  Der geplante oder auf den anderen Hosts ausgeführte Betrieb wartet auf den Abschluss des Rollbacks.

- Profile, die auf dieselbe Repository-Datenbank verweisen, müssen mit unterschiedlichen Namen in den SnapManager-Server-Hosts erstellt werden.

  Wenn Sie Profile mit demselben Namen verwenden, schlägt der Rollback-Vorgang mit dieser Repository-Datenbank ohne Warnung fehl.

- SnapManager-Vorgänge dürfen nicht auf dem Host ausgeführt werden, den Sie zurücksetzen möchten.

  Wenn ein Vorgang ausgeführt wird, müssen Sie warten, bis dieser Vorgang abgeschlossen ist, und bevor Sie mit dem Rollback fortfahren.

> Der Rollback-Vorgang wird längere Zeit ausgeführt, da sich die kumulative Anzahl von Backups der Hosts, die gemeinsam wieder erstellt werden, erhöht. Die Dauer des Rollbacks kann je nach Anzahl der Profile und Backups, die mit einem bestimmten Host verbunden sind, variieren.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Durchführen eines Rollbacks auf einem oder mehreren Hosts

Sie können auf einem oder mehreren SnapManager Server Hosts ein Rollback durchführen, indem Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Sie müssen sicherstellen, dass alle Voraussetzungen für die Durchführung eines Rollbacks abgeschlossen sind.

1. Geben Sie den folgenden Befehl ein, um ein Rollback auf einem einzelnen Host durchzuführen:

```
smorepository rollback-repository-dbnamerepo_service_name-hostrepo_host-login-
usernamerepo_username-portrepo_port-rollbackhosthost_with_target_database
```

Das folgende Beispiel zeigt den Befehl zum Rollback aller Zieldatenbanken, die auf hostA gemountet sind, und eine Repository-Datenbank namens repoA, die sich auf dem Repository-Host, repo_Host, befindet:

```
smo repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA
```

2. Um ein Rollback auf mehreren Hosts durchzuführen, geben Sie den folgenden Befehl ein: Smarorpository Rollback-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-rollbackhostost_with_Target_database1,Host_with_Target_database2

> Geben Sie bei mehreren Hosts die durch Komma getrennten Hostnamen ein, und stellen Sie sicher, dass zwischen dem Komma und dem nächsten Hostnamen kein Platz vorhanden ist.

Wenn Sie die Real Application Clusters (RAC)-Konfiguration verwenden, müssen Sie alle RAC-verbundenen Hosts manuell wiederherstellen. Sie können -allhosts verwenden, um ein Rollback aller Hosts durchzuführen.

Das folgende Beispiel zeigt den Befehl zum Rollback aller Zieldatenbanken, die auf den Hosts gemountet sind, hostA, hostB und eine Repository-Datenbank namens repoA auf dem Repository-Host, repo_Host:

```
smo repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA,hostB
```

Die Hosts, Profile, Zeitpläne, Backups und Klone, die mit den Profilen der Zieldatenbanken für den Host verbunden sind, werden in das frühere Repository zurückgesetzt.

Verwandte Informationen

Voraussetzungen für die Durchführung eines Rollbacks

Aufgaben nach dem Rollback ausführen

Sie müssen einige weitere Schritte durchführen, nachdem Sie eine Repository-Datenbank zurückgesetzt und den SnapManager-Host von SnapManager 3.2 auf SnapManager 3.0 heruntergestuft haben, um die Zeitpläne anzuzeigen, die in der früheren Version der Repository-Datenbank erstellt wurden.

1. Navigieren Sie zu cd/opt/NetApp/smo/Repositorys.

   Das Repository-Verzeichnis kann zwei Dateien für jedes Repository enthalten. Der Dateiname mit dem Zahlenzeichen (#) wird mit SnapManager 3.1 oder höher erstellt und der Dateiname mit dem Bindestrich (-) wird mit dem SnapManager 3.0 erstellt.

   Die Dateinamen können wie folgt lauten:

   - Repository#SMO300a#SMOREPO1#10.72.197.141#1521
   - Repository-smo300a-smorepo1-10.72.197.141-1521
2. Ersetzen Sie das Zahlenzeichen (#) im Dateinamen durch den Bindestrich (-).

   Der Dateiname mit dem Zahlenzeichen (#) enthält jetzt Bindestrich (-): Repository-SMO300a-SMOREPO1-10.72.197.141-1521.

SnapManager wird konfiguriert

Nach der Installation von SnapManager müssen Sie je nach verwendeter Umgebung einige zusätzliche Konfigurationsaufgaben ausführen.

SnapManager-Konfigurationsparameter

SnapManager bietet eine Liste der Konfigurationsparameter, die Sie je nach Anforderung bearbeiten können. Die Konfigurationsparameter werden in der Datei smo.config gespeichert. Die Datei smo.config enthält jedoch möglicherweise nicht alle unterstützten Konfigurationsparameter. Je nach Anforderung können Sie die Konfigurationsparameter hinzufügen.

In der folgenden Tabelle sind alle unterstützten SnapManager-Konfigurationsparameter aufgeführt und wird erläutert, wann diese Parameter verwendet werden können:

Parameter	Beschreibung
• Behalten.hourly.count • Beibehalten.hourly.duration • Behalten.monthly.count • Aufbewahrung.monatlich.Dauer	Diese Parameter legen die Aufbewahrungsrichtlinie fest, wenn Sie ein Profil erstellen. Sie können beispielsweise die folgenden Werte zuweisen:beibehalten.hourly.count = 12 Beibehalten.hourly.duration = 2 Behalten.monthly.count = 2 Aufbewahrung.monatlich.Dauer = 6

restore.secondaryAccessPolicy	Dieser Parameter definiert, wie SnapManager auf Daten im sekundären Storage zugreifen kann, wenn sie nicht direkt mithilfe von Protection Manager wiederhergestellt werden können. Folgende Möglichkeiten für den Zugriff auf Daten im sekundären Storage: • Direkt (Standard) Wenn restore.secondaryAccessPolicy auf direkt festgelegt ist, werden Daten in SnapManager auf sekundärem Storage geklont, die geklonten Daten vom sekundären Storage an den Host gemountet und dann Daten aus dem Klon in der aktiven Umgebung kopiert. • Indirekt Wenn Sie restore.secondaryAccessPolicy indirekt zuweisen, kopiert SnapManager Daten zu einem temporären Volume auf einem primären Storage, bindet Daten vom temporären Volume an den Host und kopiert dann Daten aus dem temporären Volume in die aktive Umgebung. Die indirekte Methode muss nur verwendet werden, wenn der Host keinen direkten Zugriff auf das sekundäre Speichersystem hat. Diese Methode dauert doppelt so lange wie die direkte Methode, da zwei Kopien der Daten erstellt werden. In einem Storage Area Network (SAN) mit Network File System (NFS) als Protokoll muss SnapManager keine direkte Verbindung zum sekundären Storage herstellen, um eine Wiederherstellung durchzuführen.

Restore.temporarVolumeName	Dieser Parameter weist dem temporären Volume einen Namen zu. Wenn SnapManager die indirekte Methode zur Wiederherstellung von Daten aus dem sekundären Storage verwendet, wird ein Scratch Volume auf dem primären Storage benötigt, um eine temporäre Kopie von Daten zu speichern, bis sie in die Datenbankdateien kopiert und die Datenbank wiederhergestellt wird. Es gibt keinen Standardwert. Wenn Sie keinen Wert angeben, müssen Sie einen Namen in den Wiederherstellungsbefehl eingeben, der die indirekte Methode verwendet. Sie können beispielsweise die folgenden Werte zuweisen:restore.temporaryVolumeName = smo_temp_Volume
Beibehalten.alwayFreeExpiredBackups	Mit diesem Parameter kann SnapManager Backups zum Zeitpunkt des Ablaufs und zum Zeitpunkt einer schnellen Wiederherstellung freigeben, selbst wenn die Datensicherung nicht konfiguriert ist. Dieser Parameter gibt die geschützten Backups frei, die ablaufen, und löscht die ungeschützten Backups, die ablaufen. Sie können folgende Werte zuweisen: • Richtig Wenn Sie „true“ für „exwayFreeExpiredBackups“ zuweisen, gibt SnapManager die abgelaufenen Backups frei, unabhängig davon, ob die Backups geschützt sind. Die Backups werden entweder gelöscht, wenn sie nicht geschützt sind oder wenn die geschützten Kopien auf dem sekundären Speicher ebenfalls abgelaufen sind. • Falsch Wenn Sie 'false' zum execen.alwayFreeExpiredBackup zuweisen, gibt SnapManager die abgelaufenen Backups frei, die geschützt sind.

Host.Credentials.persistent	Mit diesem Parameter kann SnapManager die Hostanmeldeinformationen speichern. Standardmäßig werden die Hostanmeldeinformationen nicht gespeichert. Die Hostanmeldeinformationen müssen jedoch gespeichert werden, wenn Sie über ein benutzerdefiniertes Skript verfügen, das auf einem Remote-Klon ausgeführt wird und Zugriff auf einen Remote-Server erfordert.Sie können das Speichern von Host-Anmeldeinformationen aktivieren, indem Sie Host.requeses.persist zuweisen. SnapManager verschlüsselt und speichert die Host-Anmeldedaten.
WiederherstellungPlanMaxFilesAbgespielt	Mit diesem Parameter können Sie die maximale Anzahl von Dateien festlegen, die in der Vorschau der Wiederherstellung angezeigt werden sollen.standardmäßig zeigt SnapManager maximal 20 Dateien in der Vorschau der Wiederherstellung an. Sie können jedoch in einen Wert größer 0 ändern. Sie können beispielsweise den folgenden Wert zuweisen: • WiederherstellungPlanMaxFilesAbgespielt = 30 Wenn Sie einen ungültigen Wert angeben, wird die Standardanzahl der Dateien angezeigt.
snapshot.list.Timeout.min	Mit diesem Parameter können Sie die Zeit in Minuten festlegen, für die SnapManager warten muss, bis der Befehl Snap list ausgeführt wird, wenn Sie SnapManager-Operationen ausführen.standardmäßig wartet SnapManager 30 Minuten. Sie können jedoch in einen Wert größer 0 ändern. Sie können beispielsweise den folgenden Wert zuweisen: • snapshot.list.Timeout.min = 40 Wenn Sie einen ungültigen Wert angeben, wird der Standardwert verwendet. Wenn die Ausführungszeit des Befehls Snap list bei jedem SnapManager-Vorgang den Wert überschreitet, der Snapshot.list.Timeout.min zugewiesen ist, schlägt der Vorgang mit einer Zeitüberschreitung fehl.

PruneIfFileExistsInOtherDestination	Mit diesem Beschneidungsparameter können Sie das Ziel der Archiv-Log-Dateien definieren. Die Archivprotokolldateien werden in mehreren Zielorten gespeichert. Beim Beschneiden von Archiv-Log-Dateien muss SnapManager das Ziel der Archiv-Log-Dateien kennen. Sie können folgende Werte zuweisen: • Wenn Sie die Archiv-Log-Dateien von einem bestimmten Ziel aus pruneIfFileExistsInOtherDestination löschen möchten, müssen Sie pruneIfFileExistsInOtherDestination false zuweisen. • Wenn Sie die Archiv-Log-Dateien von einem externen Ziel aus pruneIfFileExistsInOtherDestination löschen möchten, müssen Sie true zu pruneIfFileExistsInOtherDestination zuweisen.
prune.archivelogs.backedup.from.otherdestination	Mit diesem Beschneider-Parameter können Sie die Archivprotokolldateien, die von den angegebenen Archivprotokollzielen gesichert oder von externen Archivprotokollzielen gesichert wurden, beschneiden. Sie können folgende Werte zuweisen: • Wenn Sie die Archivprotokolldateien aus den angegebenen Zielen beschneiden und wenn die Archivprotokolldateien von den angegebenen Zielen mithilfe von -prune-dest gesichert werden, müssen Sie false prune.archivelogs.backedup.from.otherdestination zuweisen. • Wenn Sie die Archivprotokolldateien von angegebenen Zielen beschneiden und die Archivprotokolldateien mindestens einmal von einem der anderen Ziele gesichert werden sollen, müssen Sie True prune.archivelogs.backedup.from.otherdestination zuweisen.

Maximum.archivolog.files.toprune.atATIME	Mit diesem Beschneider-Parameter können Sie die maximale Anzahl von Archivprotokolldateien definieren, die Sie zu einem bestimmten Zeitpunkt beschneiden können. Sie können beispielsweise den folgenden Wert zuweisen:maximum.archivelog.files.toprune.atATIME = 998 Der Wert, der maximal.archivolog.files.toprune.atatime zugewiesen werden kann, muss kleiner als 1000 sein.
Archivprotokolle.konsolidieren	Mit diesem Parameter kann SnapManager die doppelten Archiv-Log-Backups freigeben, wenn Sie true dem archivelogs.Consolidate zuweisen.
Suffix.Backup.Label.with.logs	Mit diesem Parameter können Sie das Suffix angeben, das Sie hinzufügen möchten, um die Namen der Bezeichnungen der Datensicherung und des Archiv-Log-Backups zu unterscheiden.zum Beispiel, wenn Sie Logs dem Suffix.Backup.Label.with.logs zuweisen, wird _logs als Suffix zum Backup-Label des Archivprotokolls hinzugefügt. Das Backup-Label für das Archivprotokoll wäre dann ARCH_logs.
backup.archivelogs.beyond.missingfiles	Mit diesem Parameter kann SnapManager die fehlenden Archivprotokolldateien in die Sicherung aufnehmen. Die Archivprotokolldateien, die nicht im aktiven Dateisystem vorhanden sind, sind nicht im Backup enthalten. Wenn Sie alle Archivprotokolldateien einschließen möchten, auch jene, die nicht im aktiven Dateisystem vorhanden sind, müssen Sie True backup.archivelogs.beyond.missingfiles zuweisen. Sie können FALSE zuweisen, um die fehlenden Archivprotokolldateien zu ignorieren.
Srvctl.Timeout	Mit diesem Parameter können Sie den Timeout-Wert für den srvctl-Befehl definieren. **Hinweis:** die Serversteuerung (SRVCTL) ist ein Dienstprogramm zur Verwaltung von RAC-Instanzen. Wenn SnapManager mehr Zeit in Anspruch nimmt, um den srvctl-Befehl auszuführen als den Timeout-Wert, schlägt der SnapManager-Vorgang mit dieser Fehlermeldung fehl: Fehler: Timeout ist beim Ausführen des Befehls srvctl-Status aufgetreten.

snapshot.restore.storageNameCheck	Mit diesem Parameter kann SnapManager den Wiederherstellungsvorgang mit Snapshot Kopien durchführen, die vor der Migration von Data ONTAP im 7-Mode zu Clustered Data ONTAP erstellt wurden. Der dem Parameter zugewiesene Standardwert ist false. Wenn Sie von Data ONTAP 7-Mode zu Clustered Data ONTAP migriert haben, die Snapshot Kopien jedoch vor der Migration verwenden möchten, legen Sie den Wert für Snapshot.restore.storageNameCheck=true fest.
services.common.disableAbort	Dieser Parameter deaktiviert die Bereinigung bei einem Ausfall lang laufender Vorgänge. Wenn Sie services.common.disableAbort=true.For beispielsweise einen Klonvorgang ausführen, der lange dauert und dann aufgrund eines Oracle-Fehlers fehlschlägt, sollten Sie den Klon möglicherweise nicht bereinigen. Wenn Sie services.common.disableAbort=true festlegen, wird der Klon nicht gelöscht. Sie können das Oracle Problem beheben und den Klonvorgang ab dem Fehlerpunkt neu starten.
• Backup.Sleep.dnfs.Layout • backup.sleep.dnfs.secs	Diese Parameter aktivieren den Schlafmechanismus im Direct NFS Layout (dNFS). Nachdem Sie die Datensicherung der Kontrolldateien mit dNFS oder einem Network File System (NFS) erstellt haben, versucht SnapManager, die Kontrolldateien zu lesen, aber die Dateien werden möglicherweise nicht gefunden.um den Sleep-Mechanismus zu aktivieren, stellen Sie sicher, dass Backup.Sleep.dnfs.Layout=true. Der Standardwert ist true. Wenn Sie den Schlafmechanismus aktivieren, müssen Sie die Schlafdauer backup.sleep.dnfs.secs zuweisen. Die zugewiesene Schlafzeit ist in Sekunden und der Wert hängt von Ihrer Umgebung ab. Der Standardwert ist 5 Sekunden. Beispiel: • Backup.Sleep.dnfs.Layout=true • backup.sleep.dnfs.secs=2

• override.default.backup.pattern • new.default.backup.pattern	Wenn Sie das Backup-Label nicht angeben, erstellt SnapManager ein Standard-Backup-Label. Mit diesen SnapManager-Parametern können Sie das Standard-Backup-Label anpassen.um die Anpassung des Backup-Labels zu ermöglichen, stellen Sie sicher, dass der Wert override.default.backup.pattern auf true gesetzt ist. Der Standardwert ist false. Um das neue Muster des Backup-Labels zuzuweisen, können Sie Schlüsselwörter wie Datenbankname, Profilname, Umfang, Modus und Hostname new.default.backup.pattern zuweisen. Die Stichwörter sollten mit einem Unterstrich getrennt werden. Beispiel: new.default.backup.pattern=dbname_profile_hostname_scope_mode. Der Zeitstempel wird automatisch am Ende des generierten Etiketts eingefügt.
allow.underscore.in.clone.sid	Oracle unterstützt die Verwendung des Unterstreichung in Clone SID von Oracle 11gR2. Mit diesem SnapManager-Parameter können Sie einen Unterstrich in den Namen Clone SID einfügen.um einen Unterstrich in den Clone SID-Namen einzuschließen, stellen Sie sicher, dass der Wert allow.underscore.in.clone.sid auf true gesetzt ist. Der Standardwert ist true. Wenn Sie eine Oracle-Version vor Oracle 11gR2 verwenden oder keinen Unterstrich in den Namen Clone SID aufnehmen möchten, setzen Sie den Wert auf false.
oracle.parameters.with.comma	Mit diesem Parameter können Sie alle Oracle-Parameter angeben, die Komma (,) als Wert haben.während einer Operation verwendet SnapManager oracle.parameters.with.comma, um alle Oracle-Parameter zu überprüfen und die Aufteilung der Werte zu überspringen. Wenn z. B. der Wert von nls_numeric_characters=, angegeben wird, geben Sie dann oracle.parameters.with.comma=nls_numeric_characters an. Wenn mehrere Oracle-Parameter mit Komma als Wert vorhanden sind, müssen Sie alle Parameter in oracle.parameters.with.comma angeben.

• ArchivLogs.exclude • ArchivedLogs.exclude.fileslike • <db-unique-Name>.archivedLogs.exclude.fileslike	Diese Parameter erlauben es SnapManager, die Archivprotokolldateien von den Profilen und Backups auszuschließen, wenn sich die Datenbank nicht auf einem Speichersystem befindet, das mit Snapshot Kopien aktiviert ist, und Sie SnapManager-Vorgänge auf diesem Speichersystem ausführen möchten.**Hinweis:** vor der Erstellung eines müssen Sie die Ausschlussparameter in die Konfigurationsdatei einfügen Profil: Die diesen Parametern zugewiesenen Werte können entweder ein Verzeichnis der obersten Ebene oder ein Mount-Punkt sein, an dem die Archivprotokolldateien vorhanden sind, oder ein Unterverzeichnis. Wenn ein Verzeichnis auf der obersten Ebene oder ein Bereitstellungspunkt angegeben wird und wenn der Datenschutz für ein Profil auf dem Host aktiviert ist, ist dieser Bereitstellungspunkt oder Verzeichnis nicht in dem Datensatz enthalten, der in Protection Manager erstellt wird. Wenn mehrere Archivprotokolldateien vom Host ausgeschlossen werden sollen, müssen Sie die Pfade der Archivprotokolldatei durch Kommas trennen. Um die Archivprotokolldateien von der Integration im Profil und der Sicherung auszuschließen, müssen Sie einen der folgenden Parameter angeben: • ArchivedLogs.exclude, um einen regulären Ausdruck für das Ausschließen von Archiv-Log-Dateien aus allen Profilen oder Backups anzugeben. Die Archivprotokolldateien, die dem regulären Ausdruck entsprechen, werden von allen Profilen und Backups ausgeschlossen. Zum Beispiel können Sie archivedLogs.exclude = /arch/logs/on/local/disk1/.**,/arche/logs/On/local/disk2/.** festlegen. Für ASM-Datenbanken können Sie archivedLogs.exclude = \\+KHDB_ARCH_DEST/khdb/archivelog/.**,\\+KHDB_NONNAARCHTWO/khdb/archivelog/.** festlegen. • ArchivedLogs.exclude.filesWie geben Sie einen SQL-Ausdruck an, um Archivprotokolldateien von allen Profilen oder Backups auszuschließen. Die Archivprotokolldateien, die dem SQL-Ausdruck entsprechen, werden von allen Profilen und Backups ausgeschlossen. Sie können zum Beispiel archivedLogs.exclude.fileslike = /arch/logs/on/local/disk1/%,/arch/logs/On/local/disk2/% festlegen.

Bearbeiten der Konfigurationsparameter

Je nach Umgebung können Sie die Standardwerte ändern, die dem Konfigurationsparameter zugewiesen sind.

1. Öffnen Sie die Konfigurationsdatei vom folgenden Standardspeicherort:

   Standard Installation location/Properties/smo.config

2. Ändern Sie die Standardwerte der Konfigurationsparameter.

   Sie können auch unterstützte Konfigurationsparameter hinzufügen, die nicht in der Konfigurationsdatei enthalten sind, und ihnen Werte zuweisen.

3. Starten Sie den SnapManager für Oracle Server neu.

- <db-unique-Name>.archivedLogs.exclude.filesWie geben Sie einen SQL-Ausdruck an, um Archivprotokolldateien ausschließlich aus dem Profil oder dem Backup auszuschließen, das für die Datenbank mit dem angegebenen db-Unique-Namen erstellt wurde.

  Die Archivprotokolldateien, die dem SQL-Ausdruck entsprechen, werden vom Profil und den Backups ausgeschlossen.

  Sie können beispielsweise mydb.archivedLogs.exclude.filelike = /arch/logs/on/local/disk1/%,/arch/logs/On/local/disk2/% festlegen.

Konfiguration von SnapDrive für UNIX für eine aktiv/aktiv-Umgebung von Veritas SFRAC

Wenn Sie den Parameter Host-Cluster-sw-Restore-warn in snapdrive.conf hinzugefügt haben und den Wert an zugewiesen haben, müssen Sie den Wert ändern, um die Wiederherstellung in der aktiv/aktiv Veritas Storage Foundation for Oracle RAC (SFRAC) Umgebung zu unterstützen.

Wenn Sie die aktive/aktive Veritas Storage Foundation for Oracle RAC (SFRAC) Umgebung verwenden, wenn der Parameter Host-Cluster-sw-Restore-warn auf ein gesetzt ist, wird eine Warnmeldung angezeigt und der Wiederherstellungsvorgang wird angehalten. Wenn Sie die Wiederherstellung in einer aktiven/aktiven Veritas SFRAC Umgebung durchführen möchten, müssen Sie Host-Cluster-sw-Restore-warn auf off setzen.

Weitere Informationen auf snapdrive.conf finden Sie in der SnapDrive-Dokumentation.

1. Melden Sie sich als Root-Benutzer an.
2. Öffnen Sie die snapdrive.conf-Datei mit einem Texteditor.
3. Ändern Sie den Wert für Host-Cluster-sw-Restore-warn auf aus.

Starten Sie nach der Konfiguration den SnapDrive für UNIX-Server neu.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Konfiguration von SnapManager zur Unterstützung der Veritas SFRAC-Umgebung

Wenn SnapManager auf Solaris installiert ist, können Sie SnapManager so konfigurieren, dass die Veritas Storage Foundation for Oracle RAC-Umgebung (SFRAC) unterstützt wird.

- Auf dem Host müssen Solaris, Host Utilities und Veritas installiert sein.
  a. Erstellen Sie mithilfe von SnapDrive für UNIX eine gemeinsame Laufwerksgruppe und ein Dateisystem für SnapManager, sodass die Dateisysteme gleichzeitig auf beiden Knoten des Real Application Clusters (RAC) gemountet sind.

     Informationen zum Erstellen einer freigegebenen Laufwerksgruppe und eines Dateisystems finden Sie

in der SnapDrive-Dokumentation.

b. Installieren und konfigurieren Sie die Oracle-Datenbank, die auf den freigegebenen Dateisystemen gemountet werden soll.

c. Starten Sie eine Datenbankinstanz auf einem beliebigen Knoten des RAC.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Sicherstellen, dass ASM importierte Festplatten erkennt

Wenn Sie in einer NFS-Umgebung Automatic Storage Management (ASM) verwenden, müssen Sie nach der Installation von SnapManager sicherstellen, dass ASM die von SnapManager importierten Laufwerke erkennen kann. Dazu fügen Sie den Pfad des ASM-Verzeichnisses zum Parameter ASM_DISKSTRING hinzu.

Sie können Oracle Tools verwenden, um den Parameter ASM_DISKSTRING zu bearbeiten. Informationen zum Bearbeiten von ASM_DISKSTRING finden Sie in der Oracle-Dokumentation.

Der ASM-Festplattenpfad /opt/NetApp/smo/mnt//Disk*' muss dem vorhandenen Pfad hinzugefügt werden, der im Parameter ASM_DISKSTRING definiert ist. Wenn der Pfad in ASM_DISKSTRING beispielsweise /mnt/my-asm-Disks/dir1/Disk* definiert war, wird der aktualisierte Pfad nach dem Hinzufügen des ASM-Festplattenpfads '/mnt/my-asm-Disks/dir1/Disk*,/opt/NetApp/smo/mnt//Disk*' sein.

Der Parameter ASM_DISKSTRING muss nur mit den ASM-Festplattendateien und nicht mit anderen Dateien übereinstimmen.

- Das erste Sternchen (*) gibt den von SnapManager für den Root-Mount-Punkt generierten Namen an.
- Das zweite * zeigt das Verzeichnis innerhalb des Mount-Punkts an.
- Der dritte * gibt den Namen der NFS-Datei an.

Sie müssen sicherstellen, dass das * mit der Topologie Ihres NFS-Dateisystems übereinstimmt, wenn die Festplatte in die Verzeichnisse unter /opt/NetApp/smo/mnt/<smo-generated-Name>/ eingebunden ist.

1. Wenn Sie ASM-Disks mit NFS in der Network Attached Storage (NAS)-Umgebung verwenden, bearbeiten Sie den Parameter ASM_DISKSTRING, sodass er auf den aktuellen ASM-Verzeichnispfad zeigt.

   Wenn der Mount-Punkt für die ASM-Disks /mnt/my-asm-Disks//**Disk** ist, nach dem Bearbeiten von ASM_DISKSTRING der aktualisierte Pfad /opt/NetApp/smo/mnt/my-asm-Disks-20081012/disk1.nfs. Der Parameter ASM_DISKSTRING befindet sich in der Form /opt/NetApp/smo/mnt//**Disk**.

   - Das erste * entspricht my-asm-Disks-20081012.
   - Die Festplatte* stimmt mit disk1.nfs überein. Nach der Bearbeitung des Parameters ASM_DISKSTRING sind die Ergebnisse von ASM Erkennung der von SnapManager importierten Platten wie folgt:
   - Klon von ASM auf NFS-Festplatten1 ist /opt/NetApp/smo/mnt/-mnt-my-asm-Disks-20081012/dir1/disk1.nfs.
   - Klon von ASM auf NFS-Festplatten2 ist /opt/NetApp/smo/mnt/-mnt-my-asm-Disks-20081012/dir1/disk2.nfs. Der Parameter ASM_DISKSTRING lautet in dem Formular /opt/NetApp/smo/mnt//Disk*.
   - Die erste * stimmt -mnt-my-asm-Disks-20081012 überein.

- Das zweite * entspricht dir1.
- Das dritte * stimmt disk1.nfs und disk2.nfs überein.

2. Wenn Sie ASM-Laufwerke in der SAN-Umgebung (Storage Area Network) verwenden, führen Sie je nach Umgebung einen der folgenden Schritte aus:

Wenn Sie ASM-Disks mit verwenden…	Dann…
ASMLib über FCP und iSCSI unter Linux	Ändern Sie die Berechtigung des Oracle-Softwareigners und der primären Gruppe des Benutzers, indem Sie nur das Zeichengerät verwenden. Der Pfad ASM_DISKSTRING muss ASM DISKSTRING = ORCL:* sein.
FCP und iSCSI auf AIX	Fügen Sie den Pfadnamen für den Parameter ASM_DISKSTRING bis zum Pfad des ASM-Verzeichnisses hinzu. Der Pfad ASM_DISKSTRING muss ASM DISKSTRING = /dev/hdsk/* sein, wobei * den ASM-Festplattennamen angibt.
FCP und iSCSI auf Solaris	Fügen Sie den Pfadnamen für den Parameter ASM_DISKSTRING bis zum Pfad des ASM-Verzeichnisses hinzu. Der Pfad ASM_DISKSTRING muss ASM DISKSTRING = /dev/rdsk/* sein, wobei * den ASM-Festplattennamen angibt. +

"Oracle Dokumentation: www.oracle.com/technetwork/indexes/documentation/index.html"

Sicherheits- und Anmeldeinformationsmanagement

Die Sicherheit lässt sich in SnapManager unter Verwendung von Benutzerauthentifizierungund rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) managen. Die Benutzerauthentifizierungsmethode ermöglicht den Zugriff auf Ressourcen wie Repositorys, Hosts und Profile. RBAC ermöglicht Ihnen, die Vorgänge, die SnapManager für die Volumes und LUNs ausführen kann, die die Datendateien in der Datenbank enthalten, einzuschränken.

Wenn Sie einen Vorgang über die Befehlszeilenschnittstelle (CLI) oder die grafische Benutzeroberfläche (GUI) ausführen, ruft SnapManager die für Repositorys und Profile festgelegten Anmeldeinformationen ab. SnapManager speichert Anmeldeinformationen früherer Installationen.

Das Repository und die Profile können mit einem Passwort gesichert werden. Eine Anmeldeinformationen ist das für den Benutzer für ein Objekt konfigurierte Passwort, und das Passwort ist nicht für das Objekt selbst konfiguriert.

Sie können die Authentifizierung und Anmeldeinformationen verwalten, indem Sie die folgenden Aufgaben ausführen:

- Verwalten Sie die Benutzerauthentifizierung entweder durch Eingabeaufforderungen für Passwörter für Vorgänge oder mithilfe des Befehls smo Credential Set.

  Legen Sie Anmeldedaten für ein Repository, einen Host oder ein Profil fest.

- Zeigen Sie die Anmeldeinformationen an, die die Ressourcen regeln, auf die Sie Zugriff haben.
- Löschen Sie die Anmeldeinformationen eines Benutzers für alle Ressourcen (Hosts, Repositorys und Profile).
- Löschen Sie die Anmeldeinformationen eines Benutzers für einzelne Ressourcen (Hosts, Repositorys und Profile).

Sie können rollenbasierten Zugriff verwalten, indem Sie die folgenden Aufgaben ausführen:

- RBAC für SnapManager wird mithilfe von SnapDrive aktiviert.
- Weisen Sie Benutzer über die Operations Manager-Konsole Rollen zu und legen Sie Rollenfunktionen fest.
- Aktivieren Sie optional SnapManager zum Speichern verschlüsselter Passwörter, indem Sie die Datei smo.config bearbeiten.

Wenn Protection Manager installiert ist, wird der Zugriff auf die Funktionen wie folgt beeinträchtigt:

- Falls Protection Manager installiert ist, erstellt SnapManager bei der Erstellung eines Datenbankprofils einen Datensatz und füllt den Datensatz mit den Volumes aus, die die Datenbankdateien enthalten.

  Nach einem Backup-Vorgang synchronisiert SnapManager den Datensatz mithilfe der Datenbankdateien.

- Wenn Protection Manager nicht installiert ist, kann SnapManager keinen Datensatz erstellen und Sie können keinen Schutz für Profile festlegen.

Was ist die Benutzerauthentifizierung

Zusätzlich zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) wird der Benutzer über eine Betriebssystem-Anmeldung auf dem Host, auf dem der SnapManager Server ausgeführt wird, authentifiziert. Sie können die Benutzerauthentifizierung entweder durch Eingabeaufforderungen für Passwörter zu Vorgängen oder mithilfe des Befehls smo-Anmeldeinformationssatz aktivieren.

Die Anforderungen an die Benutzerauthentifizierung hängen davon ab, wo der Vorgang ausgeführt wird.

- Wenn sich der SnapManager-Client auf demselben Server wie der SnapManager-Host befindet, werden Sie durch die BS-Anmeldedaten authentifiziert.

  Sie werden nicht zur Eingabe eines Passworts aufgefordert, da Sie bereits beim Host angemeldet sind, auf dem der SnapManager-Server ausgeführt wird.

- Wenn der SnapManager-Client und der SnapManager-Server auf verschiedenen Hosts sind, muss SnapManager Sie mit beiden OS-Anmeldedaten authentifizieren.

  SnapManager fordert Sie zur Eingabe von Passwörtern für jeden Vorgang auf, wenn Sie Ihre BS-Anmeldeinformationen nicht im SnapManager-Benutzereinweiscache gespeichert haben. Wenn Sie den Befehl smo causendential set -Host eingeben, speichern Sie die OS-Anmeldeinformationen in der SnapManager-Anmeldeinformationscache-Datei und so fordert SnapManager nicht zur Eingabe des Passworts für einen Vorgang auf.

Wenn Sie mit dem SnapManager-Server authentifiziert sind, gelten Sie als effektiver Benutzer. Der effektive Benutzer für einen Vorgang muss ein gültiges Benutzerkonto auf dem Host sein, auf dem der Vorgang ausgeführt wird. Wenn Sie beispielsweise einen Klonvorgang ausführen, sollten Sie sich beim Ziel-Host für den Klon einloggen können.

SnapManager für Oracle kann die Autorisierung von Benutzern, die in zentralen Active Directory-Diensten erstellt wurden, z. B. LDAP und ADS, möglicherweise nicht unterstützen. Um sicherzustellen, dass die Authentifizierung nicht fehlschlägt, müssen Sie die konfigurierbare auth.diableServerAuthorization auf true setzen.

Als effektiver Benutzer können Sie die Anmeldeinformationen folgendermaßen verwalten:

- Optional können Sie SnapManager so konfigurieren, dass Benutzeranmeldeinformationen in der SnapManager-Benutzeranmeldedatei gespeichert werden.

  Standardmäßig werden in SnapManager keine Host-Anmeldedaten gespeichert. Sie können dies ändern, beispielsweise, wenn Sie benutzerdefinierte Skripte haben, die Zugriff auf einen Remote-Host benötigen. Der Remote-Klonvorgang ist ein Beispiel für eine SnapManager-Operation, die die Anmeldedaten eines Benutzers für einen Remote-Host benötigt. Um die Anmeldedaten des SnapManager-Benutzerhosts im SnapManager-Benutzeranmeldungs-Cache zu speichern, legen Sie in der Datei smo.config die Eigenschaft Host.anmeldungs.persist auf true fest.

- Sie können den Benutzerzugriff auf das Repository autorisieren.
- Sie können den Benutzerzugriff auf Profile autorisieren.
- Sie können alle Benutzeranmeldeinformationen anzeigen.
- Sie können die Anmeldeinformationen eines Benutzers für alle Ressourcen (Hosts, Repositorys und Profile) löschen.
- Anmeldedaten für einzelne Ressourcen (Hosts, Repositorys und Profile) können gelöscht werden.

Die rollenbasierte Zugriffssteuerung

Dank der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) können Sie kontrollieren, wer Zugriff auf den SnapManager Betrieb hat. Über die rollenbasierte Zugriffssteuerung können Administratoren Benutzergruppen managen, indem sie Rollen festlegen und Benutzern diese Rollen zuweisen. Nutzen Sie die SnapManager RBAC-Funktionen auch in Umgebungen, in denen die RBAC bereits vorhanden ist.

RBAC bietet die folgenden Komponenten:

- Ressourcen: Volumes und LUNs, die die Datendateien enthalten, die Ihre Datenbank ausmachen.
- Fähigkeiten: Arten von Operationen, die an einer Ressource durchgeführt werden können.
- Benutzer: Personen, denen Sie Fähigkeiten gewähren.
- Rollen: Eine Reihe von Ressourcen und Funktionen, die für Ressourcen zulässig sind. Sie weisen einem Benutzer eine bestimmte Rolle zu, der diese Funktionen ausführen soll.

Sie aktivieren die RBAC in SnapDrive. Anschließend können Sie in der grafischen Benutzeroberfläche des Operations Manager Web oder der Befehlszeilenschnittstelle bestimmte Funktionen pro Rolle konfigurieren. RBAC-Überprüfungen erfolgen auf dem DataFabric Manager Server.

In der folgenden Tabelle werden einige Rollen und ihre typischen Aufgaben aufgeführt, die in Operations

Manager festgelegt sind.

Rolle	Typische Aufgaben
Oracle Datenbankadministrator	• Erstellen, Warten und Überwachen einer Oracle-Datenbank, die sich auf einem Host befindet • Datenbank-Backups planen und erstellen • Sicherstellen, dass Backups gültig sind und wiederhergestellt werden können • Datenbanken klonen
Server-Administrator	• Einrichtung von Storage-Systemen und Aggregaten • Monitoring von Volumes für freien Speicherplatz • Bereitstellung von Storage auf Anfragen von Benutzern • Konfiguration und Monitoring von Disaster Recovery Mirroring
Storage-Architekt	• Treffen von Architekturentscheidungen beim Storage • Planung des Wachstums der Storage-Kapazität • Planung von Disaster-Recovery-Strategien • Delegieren von Fähigkeiten an Teammitglieder

Wenn RBAC verwendet wird (d. h., Operations Manager wird installiert und RBAC in SnapDrive aktiviert ist), muss der Storage-Administrator RBAC-Berechtigungen für alle Volumes und Storage-Systeme für die Datenbankdateien zuweisen.

Aktivieren der rollenbasierten Zugriffssteuerung

Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapManager wird mithilfe von SnapDrive aktiviert. Bei der Installation von SnapDrive ist die RBAC standardmäßig deaktiviert. Nachdem Sie die RBAC in SnapDrive aktiviert haben, führt SnapManager dann alle Vorgänge mit aktivierter rollenbasierter Zugriffssteuerung durch.

die snapdrive.config Datei in SnapDrive bietet viele Optionen, von denen eine die RBAC ermöglicht.

Die SnapDrive-Dokumentation enthält Details zum SnapDrive.

1. Öffnen Sie die snapdrive.conf Datei in einem Editor.
2. RBAC aktivieren, indem der Wert des parameters für die rbac-Methode von nativ in dfm geändert wird.

   Der Standardwert für diesen Parameter ist nativ, wodurch die RBAC deaktiviert wird.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Einrichten von Funktionen und Rollen für die rollenbasierte Zugriffssteuerung

Nachdem Sie die rollenbasierte Zugriffssteuerung (RBAC) für SnapManager über SnapDrive aktiviert haben, können Sie Funktionen für rollenbasierte Zugriffssteuerung und Benutzer zu Rollen hinzufügen, um SnapManager Vorgänge durchzuführen.

Sie müssen eine Gruppe im Data Fabric Manager Server erstellen und die Gruppe sowohl dem primären als auch dem sekundären Storage hinzufügen. Führen Sie folgende Befehle aus:

- dfm Group erstellen smo_grp
- dfm Group hinzufügen smo_grpprimary_Storage_System
- dfm Group, hinzufügen smo_grpsecondary_Storage_System

Damit können RBAC-Funktionen und -Rollen entweder über die Operations Manager Webschnittstelle oder die Befehlszeilenschnittstelle (CLI) des Data Fabric Manager Servers geändert werden.

In der Tabelle sind die RBAC-Funktionen aufgeführt, die für die Durchführung des SnapManager Betriebs erforderlich sind:

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC-Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Profilerstellen oder Profilaktualisierung	SD.Speicherung.Lesen (smo_grp)	SD.Storage.Read (SMO_Profile Dataset)
Profilschutz	DFM.Database.Write (smo_grp) SD.Speicherung.Lesen (smo_grp) SD.Config.Lesen (smo_grp) SD.Config.Write (smo_grp) SD.Config.Delete (smo_grp) GlobalDataProtection	Keine
Backup erstellen	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Delete (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Write (SMO_Profile-Datensatz) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Delete (SMO_Profile-Datensatz)

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC-Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Backup-Erstellung (mit DBVerify)	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Write (SMO_Profile-Datensatz) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Delete (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset)
Backup-Erstellung (mit RMAN)	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Write (SMO_Profile-Datensatz) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Delete (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset)
Backup Restore	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Write (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Snapshot.Clone (smo_grp) SD.Snapshot.Restore (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Write (SMO_Profile-Datensatz) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Delete (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset) SD.Snapshot.Restore (SMO_Profile Dataset)

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC-Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Backup löschen	SD.Snapshot.Delete (smo_grp)	SD.Snapshot.Delete (SMO_Profile-Datensatz)
Backup verifizieren	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset)
Backup-Montage	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset)
Backup nicht verfügbar	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (SMO_Profile Dataset)
Klon erstellen	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Clone (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset)
Klon löschen	SD.Snapshot.Clone (smo_grp)	SD.Snapshot.Clone (SMO_Profile Dataset)

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC-Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Aufteilung klonen	SD.Speicherung.Lesen (smo_grp) SD.Snapshot.Lesen (smo_grp) SD.Snapshot.Clone (smo_grp) SD.Snapshot.Delete (smo_grp) SD.Storage.Write (smo_grp)	SD.Storage.Read (SMO_Profile Dataset) SD.Snapshot.Read (SMO_Profile-Datensatz) SD.Snapshot.Clone (SMO_Profile Dataset) SD.Snapshot.Delete (SMO_Profile-Datensatz) SD.Storage.Write (SMO_Profile Dataset)

Details zum Definieren der RBAC-Funktionen finden Sie im *OnCommand Unified Manager Operations Manager Administration Guide*.

1. Zugriff auf die Operations Manager Konsole.
2. Wählen Sie im Menü Setup die Option **Rollen** aus.
3. Wählen Sie eine vorhandene Rolle aus, oder erstellen Sie eine neue Rolle.
4. Um den Datenbank-Speicherressourcen Vorgänge zuzuweisen, klicken Sie auf **Funktionen hinzufügen**.
5. Klicken Sie auf der Seite Rolleneinstellungen bearbeiten, um Ihre Änderungen an der Rolle zu speichern, auf **Aktualisieren**.

Verwandte Informationen

"*OnCommand Unified Manager Operations Manager Administration Guide*: mysupport.netapp.com/documentation/productsatoz/index.html"

Verschlüsselte Passwörter für benutzerdefinierte Skripts speichern

Standardmäßig speichert SnapManager keine Hostanmeldeinformationen im Cache für Benutzeranmeldeinformationen. Sie können dies jedoch ändern. Sie können die Datei smo.config bearbeiten, um die Speicherung der Hostanmeldeinformationen zu ermöglichen.

Die Datei smo.config befindet sich unter <default Installation location>/Properties/smo.config

1. Bearbeiten Sie die Datei smo.config.
2. Legen Sie Host.Credentials.persist auf true fest.

Zugriffsberechtigung für das Repository

Zusätzlich zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)

können Sie mit SnapManager Anmeldedaten für Datenbankbenutzer für den Zugriff auf das Repository festlegen. Mithilfe von Zugangsdaten können Sie den Zugriff auf die SnapManager-Hosts, Repositorys, Profile und Datenbanken einschränken oder verhindern.

Wenn Sie die Anmeldeinformationen mithilfe des Befehls „Anmeldeinformationssatz“ festlegen, werden Sie von SnapManager nicht zur Eingabe eines Passworts aufgefordert.

Sie können Benutzeranmeldeinformationen festlegen, wenn Sie SnapManager oder höher installieren.

1. Geben Sie den folgenden Befehl ein:

   'smo Anmeldeinformationssatz -Repository -dbname repo_Service_Name -Host repo_Host -Login -Benutzername repo_username [-password repo_password] -Port repo_Port'

Zugriff auf Profile wird autorisiert

Zusätzlich zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) können Sie mithilfe von SnapManager ein Passwort für ein Profil festlegen, um unbefugten Zugriff zu verhindern.

1. Geben Sie den folgenden Befehl ein: 'smo Credential Set -profile -Name profile_Name [-password password]'

Verwandte Informationen

Der Befehl Smo Credential Set

Anzeigen von Benutzeranmeldeinformationen

Sie können die Hosts, Profile und Repositorys auflisten, auf die Sie Zugriff haben.

1. Geben Sie den folgenden Befehl ein, um die Ressourcen anzuzeigen, auf die Sie Zugriff haben: `smo credential list`

Beispiel für die Anzeige von Benutzeranmeldeinformationen

In diesem Beispiel werden die Ressourcen angezeigt, auf die Sie Zugriff haben.

```
smo credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMOREPO/hotspur:1521
Host2_test_user@SMOREPO/hotspur:1521
user1_1@SMOREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]
Hosts:
Host2
Host5
```

Verwandte Informationen

Der Befehl smo Anmeldeinformationsliste

Löschen von Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile

Sie können den Cache Ihrer Anmeldeinformationen für Ressourcen (Hosts, Repositorys und Profile) löschen. Dadurch werden alle Ressourcen-Anmeldeinformationen für den Benutzer gelöscht, der den Befehl ausführt. Nach dem Löschen des Cache müssen Sie Ihre Anmeldeinformationen erneut authentifizieren, um auf diese gesicherten Ressourcen zugreifen zu können.

1. Um Ihre Anmeldeinformationen zu löschen, geben Sie den Befehl smo cridentials clear in der SnapManager-CLI ein, oder wählen Sie in der SnapManager-Benutzeroberfläche **Admin** > **Anmeldeinformationen** > **Cache löschen** aus.
2. Schließen Sie die SnapManager-Benutzeroberfläche.

   HINWEIS:

   - Wenn Sie den Anmeldeinformationscache von der SnapManager-GUI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche nicht beenden.
   - Wenn Sie den Anmeldeinformationscache von der SnapManager-CLI gelöscht haben, müssen Sie die SnapManager-GUI neu starten.
   - Wenn Sie die verschlüsselte Anmeldedatei manuell gelöscht haben, müssen Sie die SnapManager-GUI erneut starten.
3. Um die Anmeldeinformationen erneut festzulegen, wiederholen Sie den Vorgang, um die Anmeldeinformationen für das Repository, den Profilhost und das Profil festzulegen. Weitere Informationen zum erneuten Einstellen der Benutzeranmeldeinformationen finden Sie unter „Anmeldeinformationen nach dem Löschen des Anmeldeinformationscache festlegen“.

Verwandte Informationen

Der Befehl smo Credential Clear

Einrichtung von Anmeldeinformationen nach Löschen des Anmeldeinformationscache

Nachdem Sie den Cache gelöscht haben, um die gespeicherten Benutzeranmeldeinformationen zu entfernen, können Sie die Anmeldeinformationen für die Hosts, Repositorys und Profile festlegen.

Sie müssen sicherstellen, dass Sie die gleichen Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil festlegen, das Sie zuvor angegeben haben. Beim Festlegen der Benutzeranmeldeinformationen wird eine verschlüsselte Anmeldedatei erstellt.

Die Zugangsdaten finden Sie unter /root/.netapp/smo/3.3.0.

Führen Sie in der grafischen Benutzeroberfläche von SnapManager (GUI) die folgenden Schritte aus, wenn unter „Repositories“ kein Repository vorhanden ist:

1. Klicken Sie auf **Tasks** > **vorhandenes Repository hinzufügen**, um ein vorhandenes Repository hinzuzufügen.
2. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für das Repository festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf das Repository und wählen Sie **Öffnen**.
   b. Geben Sie im Fenster Repository Credentials Authentication die Benutzeranmeldeinformationen ein.
3. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für den Host festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf den Host unter dem Repository und wählen Sie **Öffnen**.
   b. Geben Sie im Fenster Host Credentials Authentication die Benutzeranmeldeinformationen ein.
4. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für das Profil festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf das Profil unter dem Host und wählen Sie **Öffnen**.
   b. Geben Sie im Fenster Authentifizierung für Profilanmeldeinformationen die Benutzeranmeldeinformationen ein.

Löschen von Anmeldeinformationen für einzelne Ressourcen

Sie können die Anmeldeinformationen für eine der gesicherten Ressourcen löschen, z. B. ein Profil, ein Repository oder einen Host. Auf diese Weise können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt die Anmeldeinformationen des Benutzers für alle Ressourcen zu löschen.

Verwandte Informationen

Der Befehl zum Löschen von Smo-Anmeldeinformationen

Benutzeranmeldeinformationen für Repositories werden gelöscht

Sie können die Anmeldeinformationen löschen, damit ein Benutzer nicht mehr auf ein bestimmtes Repository zugreifen kann. Mit diesem Befehl können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt die Anmeldeinformationen des Benutzers für alle Ressourcen zu löschen.

1. Um Repository-Anmeldeinformationen für einen Benutzer zu löschen, geben Sie folgenden Befehl ein: 'smo Credential delete -Repository-dbnamerepo_Service_Name-hostrepo_Host-Login

-usernamerepo_username-portrepo_Port'

Löschen von Benutzeranmeldeinformationen für Hosts

Sie können die Anmeldeinformationen für einen Host löschen, sodass ein Benutzer nicht mehr darauf zugreifen kann. Mit diesem Befehl können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt alle Benutzeranmeldeinformationen für alle Ressourcen zu löschen.

1. Um die Hostanmeldeinformationen für einen Benutzer zu löschen, geben Sie den folgenden Befehl ein: 'sMo requelts delete -Host-nameHost_Name-username-username'

Benutzeranmeldeinformationen für Profile werden gelöscht

Sie können die Benutzeranmeldeinformationen für ein Profil löschen, damit ein Benutzer nicht mehr darauf zugreifen kann.

1. Um die Profilanmeldeinformationen für einen Benutzer zu löschen, geben Sie den folgenden Befehl ein: 'smo requeltion delete -profile-nameprofile_Name'

Profilverwaltung für effiziente Backups

Sie müssen in SnapManager ein Profil für die Datenbank erstellen, auf der Sie einen Vorgang ausführen möchten. Sie müssen das Profil auswählen und dann den Vorgang auswählen, den Sie durchführen möchten.

Aufgaben im Zusammenhang mit Profilen

Sie können die folgenden Aufgaben ausführen:

- Erstellung von Profilen für vollständige oder teilweise Backups und Backups auf primärem, sekundärem oder gar tertiärem Storage

  Sie können auch Profile erstellen, um die Archiv-Log-Backups von den Backups der Datendatei zu trennen.

- Verifizieren von Profilen:
- Profile aktualisieren.
- Profile löschen.

Info zu Profilen und Authentifizierung

Wenn Sie ein Profil erstellen, können Sie eine Datenbank angeben und eine der folgenden Methoden zur Verbindung mit der Datenbank auswählen:

- Oracle-Authentifizierung mit Benutzername, Passwort und Port
- Betriebssystemauthentifizierung (OS) ohne Benutzername, Passwort oder Port

  Für die OS-Authentifizierung müssen Sie die Informationen für den OS-Kontobenutzer und -Gruppen eingeben.

Um die OS-Authentifizierung für die RAC-Datenbanken (Real Application Cluster) zu verwenden, muss der SnapManager-Server auf jedem Knoten der RAC-Umgebung ausgeführt werden. Das Datenbankkennwort muss für alle Oracle-Instanzen in einer RAC-Umgebung identisch sein. SnapManager verwendet den Datenbankbenutzernamen und das Kennwort, um eine Verbindung zu jeder RAC-Instanz im Profil herzustellen.

- Datenbank-Authentifizierung, wenn sqlnet.authentication_services auf „KEINE“ eingestellt ist. SnapManager verwendet dann für alle Verbindungen zur Zieldatenbank den Datenbankbenutzernamen und das Kennwort.

Um die Datenbankauthentifizierung für eine ASM-Instanz (Automatic Storage Management) zu verwenden, müssen Sie den Benutzernamen und das Kennwort eingeben, mit dem Sie sich bei der ASM-Instanz anmelden.

Sie können sqlnet.authentication_services auf NONE nur in den folgenden Umgebungen einstellen:

Datenbank-Layout	Oracle Version	Wird die Datenbankauthentifizierung für die Zieldatenbank unterstützt	Wird die Datenbankauthentifizierung für die ASM-Instanz unterstützt
Alle nicht-ASM- und nicht-RAC-Datenbanken	Oracle 10g und Oracle 11g (weniger als 11.2.0.3)	Ja.	Nein
Eigenständige ASM-Datenbank auf UNIX	Oracle 11.2.0.3 und höher	Ja.	Ja.
ASM-Instanz auf RAC-Datenbank auf UNIX	Oracle 11.2.0.3	Nein	Nein
RAC Datenbank auf NFS	Oracle 11.2.0.3	Ja.	Nein

Hinweis: Nachdem Sie sqlnet.authentication_services deaktiviert haben und die Authentifizierungsmethode in die Datenbankauthentifizierung ändern, müssen Sie sqlnet.authentication_services auf KEINE einstellen.

Wenn Sie zum ersten Mal auf ein Profil zugreifen, müssen Sie Ihr Profilkennwort eingeben. Nachdem Sie Ihre Anmeldedaten eingegeben haben, können Sie die Datenbank-Backups im Profil anzeigen.

Verwandte Informationen

Welche Profile sind

Profile werden erstellt

Beim Erstellen von Profilen können Sie dem Profil ein bestimmtes Oracle-Datenbankbenutzerkonto zuweisen. Sie können die Aufbewahrungsrichtlinie für das Profil festlegen,Backup-Schutz für alle Backups, die dieses Profil verwenden, auf sekundärem Speicher aktivieren und für jede Aufbewahrungsklasse die Anzahl und Dauer der Aufbewahrung festlegen.

Wenn Sie die Werte der Parameter -Login, -password und -Port der Datenbank nicht angeben, verwendet der Authentifizierungsmodus des Betriebssystems die Standardanmeldeinformationen.

Während der Erstellung eines Profils führt SnapManager eine Überprüfung der Berechtigung zur Wiederherstellung durch, um den Wiederherstellungsmechanismus zu bestimmen, mit dem die Datenbank wiederhergestellt werden kann. Wenn sich die Datenbank auf einem qtree befindet und das übergeordnete Volume nicht für eine schnelle oder Volume-basierte Wiederherstellung qualifiziert ist, kann die Analyse falsch sein.

Mit SnapManager (3.2 oder höher) können Sie Archivprotokolldateien von den Datendateien trennen, während Sie ein neues Profil erstellen oder ein vorhandenes Profil aktualisieren. Nachdem Sie die Sicherung mit dem Profil getrennt haben, können Sie entweder nur die Datendateien-only-Backup oder Archiv-Log-only-Backup der Datenbank erstellen. Sie können das neue Profil oder das aktualisierte Profil verwenden, um das Backup zu erstellen, das sowohl die Datendateien als auch die Archivprotokolldateien enthält. Sie können das Profil jedoch nicht zum Erstellen der vollständigen Sicherung oder zum Zurücksetzen der Einstellungen verwenden.

Profile zur Erstellung vollständiger und partieller Backups

Sie können Profile erstellen, um das vollständige Datenbank-Backup mit den Datendateien, Kontrolldateien, Archivprotokolldateien und partiellen Datenbank-Backups zu erstellen, die bestimmte Datendateien oder Tablespaces enthalten, alle Kontrolldateien und alle Archivprotokolldateien. SnapManager erlaubt Ihnen nicht, mithilfe der Profile, die für vollständige und teilweise Backups erstellt wurden, separate Archiv-Log-Backups zu erstellen.

Profile zur Erstellung von nur-Datendateien-Backups und nur archivalogs-Backups

Wenn Sie ein neues Profil erstellen, können Sie -separatem-archivlog-Backups einbeziehen und das Archiv-Log-Backup von der Datendatei-Sicherung trennen. Sie können das vorhandene Profil auch aktualisieren, um die Sicherung des Archivprotokolls von der Datensicherung der Datendatei zu trennen.

Mithilfe der neuen Profiloptionen können Sie die Backups des Archivprotokolls trennen und folgende SnapManager-Vorgänge durchführen:

- Erstellen Sie eine Backup-Datei für Archivprotokolle
- Löschen Sie eine Sicherung des Archivprotokolls
- Mounten Sie ein Backup für das Archivprotokoll
- Kostenlose Backup eines Archivprotokolls

Während das Profil erstellt wird, um Archiv-Log-Backups von der Datensicherung zu trennen, wenn die Archiv-Log-Dateien nicht in der Datenbank vorhanden sind, für die das Profil erstellt wird, dann ist eine Warnung Archived Log-Datei nicht im aktiven Dateisystem vorhanden. Die Versionen der archivierten Protokolldatei, die früher als die Version des <Archiv-Log-Threads> -Protokolls waren, werden nicht in die Sicherung aufgenommen. Selbst wenn Sie Backups für diese Datenbank erstellen, sind die Archiv-Log-Dateien in den Datenbank-Backups nicht verfügbar.

Wenn beim Erstellen eines Profils ein Fehler auftritt, verwenden Sie den Befehl „Smosystem dump“. Nachdem Sie ein Profil erstellt haben, verwenden Sie die Befehle Smooperation dump und smoprofile dump, wenn Sie einen Fehler haben.

1. Um ein Profil mit einem Benutzernamen, Kennwort und Port (Oracle-Authentifizierung) zu erstellen, geben Sie den folgenden Befehl ein: 'smo-profile create -profileprofil [-profile-passwordprofile_password] -Repository-dbnamerepo_dbname-hostrepo_Host-portrepo_Port-Login-usernamerepo_username -Database-dbnamepo_countname [-countname {] [-{ countname-durmcountmpromationsm} } [-] [-

bussnasminosmamnesmprom] [-adym] [-bussnmpromnmnmnmprompromnmnmpromnmnmprop] [-budbm] [-adname [-assestory [-assasmommnmnmnmnmnecym] [-assestory] [-bucturmbasmasmasmasmin [-adym] [-budbm] [-budbm] [-bussmprop [-buttnmasminascommprop] [-adym [-bu

Weitere Optionen für diesen Befehl:

'[-Force] [-noprompt]'

'[leise/ausführlich]'

Für Real Application Clusters (RAC)-Umgebungen müssen Sie beim Erstellen eines neuen Profils den Wert des parameters db_Unique_Name als db_dbname angeben.

Je nach Zugriffsart auf die Datenbank können Sie auch weitere Optionen bei der Erstellung von Profilen berücksichtigen.

Wenn…	Dann…
Sie wollen die Betriebssystemauthentifizierung verwenden, um das Profil zu erstellen	Geben Sie die Variablen für ein Betriebssystemkonto in der DBA-Gruppe an (normalerweise das Konto, das für die Installation von Oracle verwendet wird). Geben Sie Folgendes an, anstatt den Benutzernamen, das Passwort und den Port hinzuzufügen: • -Oscaleraccount_Name als Name des Betriebssystemkontos • -Oscupogroup als die Gruppe, die mit dem Betriebssystem-Konto verknüpft ist
Sie möchten die Authentifizierung der Automatic Storage Management (ASM)-Instanz verwenden, um das Profil zu erstellen	Geben Sie die Anmeldeinformationen für die Authentifizierung der ASM-Instanz an. • -Asmusernameasmintance_username ist der Benutzername, der zur Anmeldung bei der ASM-Instanz verwendet wird. • -Asmpasswordasminstance_password ist das Passwort, das zur Anmeldung bei der ASM-Instanz verwendet wird.
Sie möchten die Datenbankauthentifizierung verwenden, um ein Profil zu erstellen	Geben Sie die Anmeldedaten für die Datenbank an. Wenn das Passwort Sonderzeichen wie Ausrufezeichen (!), Dollarzeichen (€) oder grave Akzent (`) enthält, dann SnapManager können Sie das authentifizierte Datenbankprofil nicht über die Befehlszeilenschnittstelle (CLI) erstellen.

Sie verwenden einen Katalog als Oracle Recovery Manager (RMAN) Repository	Geben Sie die folgenden Optionen und Variablen an: • -Nsnametnsname als der in der Datei nsnames.ora definierte tnsname. • -Login -usernameBenutzername als Benutzername, der für die Verbindung zum RMAN-Katalog erforderlich ist. Wenn nicht angegeben, verwendet SnapManager die Authentifizierungsdaten des Betriebssystems. Sie können die Betriebssystemauthentifizierung nicht mit RAC-Datenbanken verwenden. • -Passwordpassword als RMAN-Kennwort für die Verbindung mit dem RMAN-Katalog.
Sie verwenden die Steuerdatei als RMAN-Repository	Geben Sie die Option -controlfile an.
Sie wollen eine Backup Retention Policy für Backups angeben	Geben Sie entweder den Aufbewahrungszähler oder die Dauer für eine Aufbewahrungsklasse oder beides an. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). • -Hourly ist die stündliche Aufbewahrungsklasse, für die [-count n] [-duration m] der Aufbewahrungszähler und die Aufbewahrungsdauer sind, bzw.. • -Daily ist die tägliche Aufbewahrungsklasse, für die [-count n] [-durationm] die Aufbewahrungszahl und Aufbewahrungsdauer sind, bzw.. • -Weekly ist die wöchentliche Aufbewahrungsklasse, für die [-count n] [-duration m] der Aufbewahrungszähler und die Aufbewahrungsdauer sind, bzw.. • -Monthly ist die monatliche Aufbewahrungsklasse, für die [-count n] [-durationm] der Aufbewahrungszähler und die Aufbewahrungsdauer sind, bzw..

Sie wollen den Sicherungsschutz für das Profil aktivieren	Geben Sie die folgenden Optionen und Variablen an: • -Protect ermöglicht Backup-Schutz. Wenn Sie Data ONTAP in 7-Mode verwenden, erstellt diese Option einen Applikationsdatensatz im Data-Fabric-Manager-Server (DFM) und fügt Mitglieder hinzu, die sich auf die Datenbank, Datendatei, Kontrolldateien und Archivprotokolle beziehen. Wenn der Datensatz bereits vorhanden ist, wird derselbe Datensatz beim Erstellen eines Profils verwendet. • -Protection-Policy erlaubt Ihnen die Festlegung der Schutzrichtlinie. Wenn Sie Data ONTAP in 7-Mode verwenden und SnapManager mit Protection Manager integriert ist, müssen Sie eine der Protection Manager-Richtlinien angeben. Um die möglichen Schutzrichtlinien aufzulisten, verwenden Sie den Befehl smo Protection-Policy list. Wenn Sie Clustered Data ONTAP verwenden, müssen Sie entweder *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* auswählen. Der Vorgang zum Erstellen des Profils schlägt in den folgenden Szenarien fehl: ◦ Wenn Sie Clustered Data ONTAP verwenden, wählen Sie aber Protection Manager-Richtlinie aus ◦ Wenn Sie Data ONTAP in 7-Mode verwenden, wählen Sie jedoch entweder *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* Policy ◦ Wenn Sie SnapMirror Beziehung erstellt, aber *SnapManager_cDOT_Vault* Richtlinie ausgewählt oder SnapVault Beziehung erstellt haben, aber eine *SnapManager_cDOT_Mirror* Richtlinie ausgewählt haben ◦ Wenn Sie keine SnapMirror oder SnapVault Beziehung erstellt haben, sondern entweder *SnapManager_cDOT_Vault* oder *SnapManager_cDOT_Mirror* Richtlinie ausgewählt haben

Sie möchten die E-Mail-Benachrichtigung für den Abschlussstatus der Datenbankvorgänge aktivieren	Geben Sie die folgenden Optionen und Variablen an: • -Summary-notification ermöglicht Ihnen die Konfiguration einer E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank. • -Notification ermöglicht Ihnen, eine E-Mail-Benachrichtigung über den Status des Datenbankvorgangs für ein Profil zu erhalten. • -Success-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung über den erfolgreichen Datenbankvorgang zu erhalten, der mit einem neuen oder vorhandenen Profil durchgeführt wird. • -Failure-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung über den fehlgeschlagenen Datenbankvorgang zu erhalten, der mit einem neuen oder vorhandenen Profil durchgeführt wird. • -Subjectsubject_Text gibt den Subjekttext für die E-Mail-Benachrichtigung an, während ein neues Profil oder ein vorhandenes Profil erstellt wird. Wenn die Benachrichtigungseinstellungen nicht für das Repository konfiguriert sind und Sie versuchen, Profile- oder Übersichtsbenachrichtigungen mithilfe der CLI zu konfigurieren, wird die folgende Meldung im Konsole-Protokoll protokolliert: 'SMO-14577: Benachrichtigungseinstellungen nicht konfiguriert.' Wenn Sie die Benachrichtigungseinstellungen konfiguriert haben und versuchen, eine zusammenfassende Benachrichtigung mithilfe der CLI zu konfigurieren, ohne dass eine zusammenfassende Benachrichtigung für das Repository aktiviert wird, wird die folgende Meldung im Konsole-Protokoll angezeigt: 'SMO-14575: Konfiguration der zusammenfassenden Benachrichtigung für dieses Repository nicht verfügbar_'

Sie wollen Archivprotokolldateien getrennt von Datendateien sichern	Geben Sie die folgenden Optionen und Variablen an: • -Separate-archivlog-Backups ermöglicht es Ihnen, das Archiv-Log-Backup vom Datendatei-Backup zu trennen. • -Retention-archivlog-Backups legt die Aufbewahrungsdauer für Archiv-Log-Backups fest. Sie müssen eine positive Aufbewahrungsdauer angeben. Die Backups für das Archivprotokoll werden basierend auf der Aufbewahrungsdauer des Archivprotokolls aufbewahrt. Die Backups der Datendateien werden gemäß den bestehenden Aufbewahrungsrichtlinien beibehalten. • -Protect bietet Schutz für die Archiv-Log-Backups. • -Protection-Policy legt die Schutzrichtlinie auf die Archiv-Log-Backups. Die Backups für das Archivprotokoll werden anhand der Sicherungsrichtlinie für das Archivprotokoll gesichert. Die Backups der Datendateien werden auf Basis der vorhandenen Sicherungsrichtlinien gesichert. • -Include-with-Online-Backups beinhalten das Archiv-Log-Backup zusammen mit dem Online-Datenbank-Backup. Mit dieser Option können Sie ein Backup- und Archivprotokoll für Online-Datendateien zum Klonen erstellen. Wenn diese Option eingestellt ist, werden bei jeder Erstellung eines Backups von Online-Datendateien die Archiv-Logs-Backups zusammen mit den Datendateien sofort erstellt. • -No-include-with-Online-Backups beinhalten nicht das Archiv-Log-Backup zusammen mit dem Datenbank-Backup.
Nach der erfolgreichen Profilerfassungsoperation können Sie die Dump-Dateien sammeln	Geben Sie die -dump-Option am Ende des Befehls zum Erstellen von Profilen an.

Wenn Sie ein Profil erstellen, analysiert SnapManager die Dateien, falls Sie später eine Volume-basierte Wiederherstellung auf den im Profil angegebenen Dateien durchführen möchten.

Verwandte Informationen

Benennen von Snapshot-Kopien

Sie können eine Namenskonvention oder ein Muster angeben, um die Snapshot Kopien in Bezug auf das Profil zu beschreiben, das Sie erstellen oder aktualisieren. Sie können auch benutzerdefinierten Text in alle Namen von Snapshot Kopien einfügen.

Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster wird nur für Snapshot Kopien angewendet, die noch nicht aufgetreten sind. Snapshot Kopien, die vorhanden sind und das frühere Snapshot-Namensmuster behalten.

In den folgenden Beispielen werden die beiden Namen von Snapshot Kopien aufgeführt, die für ein Volume erstellt wurden. Die zweite aufgeführte Snapshot Kopie befindet sich mitten in seinem Namen *F_H_1*. Die „1“ gibt an, dass es die erste Snapshot-Kopie ist, die im Backup-Satz erstellt wurde. Die erste aufgeführte Snapshot Kopie ist der neueste und verfügt über eine „2“. Dies bedeutet, dass es sich um die zweite erstellte Snapshot Kopie handelt. Die „1“ Snapshot Kopie enthält die Datendateien; die Snapshot Kopie „2“ enthält die Kontrolldateien. Da nach der Snapshot Kopie der Datendatei Snapshot Kopien der Kontrolldatei Snapshot Kopien erstellt werden müssen, sind zwei Snapshot Kopien erforderlich.

```
smo_profile_sid_f_h_2_8ae482831ad14311011ad14328b80001_0
smo_profile_sid_f_h_1_8ae482831ad14311011ad14328b80001_0
```

Das Standardmuster enthält das erforderliche smid, wie im Folgenden dargestellt:

'* Standardmuster: smo_{Profile}_{db-sid}_{Scope}_{Mode}_{smid} * Beispiel: smo_my_Profile_rac51_f_h_2_8abc01e915a55ac50115a55a55ac8d0001_0'

Im Namen der Snapshot Kopie können Sie die folgenden Variablen verwenden:

Variablenname	Beschreibung	Beispielwert
smid (erforderlich)	Die eindeutige SnapManager-ID ist das einzige erforderliche Element, wenn ein Name für die Snapshot Kopie erstellt wird. Mit dieser ID wird sichergestellt, dass Sie einen eindeutigen Snapshot-Namen erstellen.	8abc01e915a55ac50115a55acc8d0001_0
Klasse (optional)	Aufbewahrungsklasse im Zusammenhang mit dem Backup für das Profil und angezeigt durch Stunden (h), täglich (d), wöchentlich (w), monatlich (m) oder unbegrenzt (U).	d

Kommentar (optional)	Kommentar zum Backup für das Profil. Leerzeichen in diesem Feld werden in Unterstriche konvertiert, wenn der Name der Snapshot Kopie abgeschlossen ist.	Sample_comment_Spaces_ersetzte
Datum (optional)	Datum, an dem das Backup für das Profil durchgeführt wird. Datumswerte werden bei Bedarf mit Nullen aufgefüllt. (jjjjmmtt)	20070218
db-Host (optional)	Datenbank-Host-Name, der dem Profil zugeordnet ist, das erstellt oder aktualisiert wird.	Mein_Host
db-Name (optional)	Dem von Ihnen erstellten Snapshot-Kopie zugeordneten Datenbanknamen.	rac5
db-sid (optional)	Der von Ihnen erstellten Snapshot Kopie zugeordnete Datenbank-sid.	Renn51
Beschriftung (optional)	Mit der Sicherung für das Profil verknüpfte Bezeichnung.	Sample_Label
Modus (optional)	Gibt an, ob die Sicherung online (h) oder offline (c) abgeschlossen ist.	H
Profil (optional)	Profilname, der dem von Ihnen erstellten Backup zugeordnet ist.	My_Profile
Umfang (optional)	Gibt an, ob das Backup entweder voll (f) oder partiell (p) ist.	f
Zeit (optional)	Die Dauer des Backups für das Profil. Zeitwerte für diese Variable Verwenden Sie die 24-Stunden-Uhr und werden bei Bedarf mit Nullen gepolstert. Beispielsweise werden 5:32 und 8 Sekunden als 053208 (hhhmmss) angezeigt.	170530
Zeitzone (optional)	Für den Ziel-Datenbank-Host angegebene Zeitzone.	GESCHÄTZT
Benutzertext (optional)	Benutzerdefinierter Text, den Sie eingeben können.	Prod

Hinweis: SnapManager für Oracle unterstützt das Doppelpunkt (:) Symbol in den langen Formen der Namen

für Snapshot Kopien nicht.

Profile werden umbenannt

Mit SnapManager können Sie das Profil umbenennen, wenn Sie das Profil aktualisieren. Die SnapManager Funktionen, die in dem Profil festgelegt werden, sowie die vor der Umbenennung durchzuführenden Vorgänge werden, werden für das umbenannte Profil beibehalten.

- Sie müssen sicherstellen, dass während der Umbenennung des Profils keine SnapManager-Vorgänge auf dem Profil ausgeführt werden.

Sie können das Profil sowohl von der SnapManager Befehlszeilenschnittstelle (CLI) als auch von der grafischen Benutzeroberfläche (GUI) umbenennen. Bei der Aktualisierung des Profils überprüft und aktualisiert SnapManager den Profilnamen im Repository.

SnapManager unterstützt das Umbenennen des Profils im Fenster Multi-Profile-Update nicht.

Wenn Sie einen neuen Profilnamen angeben, wird der neue Profilname im Client-seitigen Anmeldeinformationcache hinzugefügt und der frühere Profilname wird entfernt. Wenn Sie das Profil von einem Client umbenennen, wird der Anmeldeinformationscache nur von diesem Client aktualisiert. Sie müssen den Befehl smoprofile SYNC von jedem der Clients ausführen, um den neuen Anmeldeinformationscache mit dem neuen Profilnamen zu aktualisieren.

Sie können das Passwort für das Profil mithilfe des Befehls smo Credential Set festlegen.

Wenn der Profilname in einem Benennungsmuster für die Snapshot Kopie enthalten war, wird beim Umbenennen eines Profils der neue Name für das Profil aktualisiert. Alle SnapManager-Vorgänge, die im Profil ausgeführt werden, verwenden den neuen Profilnamen. Die mit einem früheren Profil erstellten Backups besitzen weiterhin den früheren Profilnamen und werden zur Durchführung anderer SnapManager Vorgänge verwendet.

Wenn Sie ein Rolling Upgrade für SnapManager-Server-Hosts durchführen, müssen Sie sicherstellen, dass Sie das gesamte Upgrade durchführen, bevor Sie das Profil umbenennen.

Der neue Name für das Profil wird nur von dem SnapManager-Client aktualisiert, aus dem die Anforderung stammt. Die SnapManager-Clients, die mit dem SnapManager-Server verbunden sind, werden nicht über die Änderung des Profilnamens benachrichtigt. Sie können das Betriebsprotokoll überprüfen, um über die Änderung des Profilnamens zu informieren.

Wenn ein geplanter Backup-Vorgang zum Zeitpunkt der Umbenennung des Profils beginnt, schlägt der geplante Vorgang fehl.

1. Geben Sie den folgenden Befehl ein: 'smo profile Update -profileprofile [-New-profilenew_profile_Name]'

Profilkennwörter werden geändert

Um die vorhandenen Profile im Repository zu schützen, sollten Sie die Passwörter für die Profile aktualisieren. Sie können dieses aktualisierte Passwort anwenden, wenn Sie ein Backup mit diesem Profil erstellen.

1. Um das Profilpasswort für ein vorhandenes Profil zu aktualisieren, geben Sie den folgenden Befehl ein:

'smo Profile Update -profile_Name -profile-password'

Verwandte Informationen

Der Befehl smoprofile Update

Profilkennwort wird zurückgesetzt

Sie können das Profilkennwort zurücksetzen, wenn Sie sich nicht an das Passwort erinnern, das Sie beim Erstellen des Profils angegeben haben.

- Sie müssen sicherstellen, dass der SnapManager-Server auf der Repository-Datenbank ausgeführt wird.
- Sie müssen über die Anmeldedaten des Root-Benutzers für den Host verfügen, auf dem sich die Repository-Datenbank befindet.
- Sie müssen sicherstellen, dass das Profil nicht für einen Vorgang verwendet wird, wenn das Passwort für dieses Profil zurückgesetzt wird.

Sie können das Passwort entweder von der SnapManager-CLI oder von der GUI aus zurücksetzen. Beim Zurücksetzen des Passworts fragt SnapManager den SnapManager-Server auf dem Repository-Host ab, um das Betriebssystem für den Repository-Host zu identifizieren. Sie müssen die Anmeldeinformationen für den autorisierten Benutzer für die Verbindung zum Repository-Host eingeben. Der SnapManager-Server authentifiziert Benutzer mit ihren Root-Anmeldedaten auf der Repository-Datenbank. Wenn die Authentifizierung erfolgreich ist, setzt SnapManager das Profilkennwort auf dem SnapManager-Server mit dem neuen Passwort zurück.

SnapManager führt den Verlauf der Vorgänge zum Zurücksetzen von Passwörtern nicht aus.

1. Zurücksetzen des Profilpassworts durch Eingabe des folgenden Befehls: 'smo password Reset -profilprofile [-profile-passwordprofile_password] [-Repository-hostadmin-passwordadmin_password]'

Zugriff auf Profile wird autorisiert

Zusätzlich zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) können Sie mithilfe von SnapManager ein Passwort für ein Profil festlegen, um unbefugten Zugriff zu verhindern.

1. Geben Sie den folgenden Befehl ein: 'smo Credential Set -profile -Name profile_Name [-password password]'

Verwandte Informationen

Der Befehl Smo Credential Set

Profile werden überprüft

Sie können überprüfen, ob ein vorhandenes Profil korrekt eingerichtet wurde. Wenn Sie ein Profil überprüfen, überprüft SnapManager die Umgebung auf das von Ihnen angegebene Profil und überprüft, ob das Profil eingerichtet ist und auf die Datenbank in diesem Profil zugegriffen werden kann.

1. Um zu überprüfen, ob das Profil ordnungsgemäß eingerichtet ist, geben Sie folgenden Befehl ein: `smo profile verify -profile profile_name`

Verwandte Informationen

Der Befehl smoprofile verify

Profile werden aktualisiert

Sie können die Profile aktualisieren, um das Profilkennwort, die Anzahl der zu behaltenden Backups, den Zugriff auf die Datenbank, die Betriebssystemauthentifizierung (OS) auf die Datenbankauthentifizierung und umgekehrt sowie Informationen zum Host zu ändern. Wenn sich die Kennwortinformationen der Oracle-Datenbank ändern, müssen Sie diese Informationen auch im Profil ändern.

Wenn die Schutzrichtlinie für das Profil aktiviert ist, kann die Richtlinie nicht über SnapManager geändert werden. Der Storage-Administrator muss die Richtlinie über die Konsole von Protection Manager ändern.

Mit SnapManager (3.2 oder höher) können Sie das Profil aktualisieren und die Archiv-Log-Backups von den Datensicherungen der Datendatei trennen, indem Sie die Option -separatem-archivlog-Backups verwenden. Sie können eine separate Aufbewahrungsdauer und eine Sicherungsrichtlinie für das Backup des Archivprotokolls festlegen. Mit SnapManager können Sie das Archivprotokoll-Backup zusammen mit dem Online-Datenbank-Backup einbeziehen. Außerdem können Sie zum Klonen eine Online-Datendatei-Backup- und ein Archivprotokoll-Backup erstellen. Wenn Sie eine Sicherung von Online-Datendateien erstellen, werden die Archivprotokolle sofort zusammen mit den Datendateien erstellt.

1. Geben Sie den folgenden Befehl ein: `smo profile update -profileprofile [-new-profilenew_profile_name] [-profile-passwordprofile_password][-database-dbnamedb_dbname-host db_host [-siddb_sid] [-login -usernamedb_username -password db_password-port db_port][-asminstance-asmusernameasminstance_username-asmpasswordasminstance_password]] [{-rman{-controlfile | {-login -usernamerman_username-password rman_password-tnsname rman_tnsname}}} | -remove-rman]-osaccountosaccount-osgrouposgroup [-retain [-hourly [-countn] [-durationm]] [-daily [-countn] [-durationm]] [-weekly [-countn] [-durationm]] [-monthly [-countn] [-durationm]]] [-commentcomment][-snapname-patternpattern][[-protect [-protection-policypolicy_name]]| [[-noprotect]] [-summary-notification] [-notification [-success-emailemail_address1, email_address2-subjectsubject_pattern] [-failure-emailemail_address1, email_address2-subjectsubject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hourshours | -daysdays | -weeksweeks| -monthsmonths [-protect [-protection-policypolicy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]`

   Weitere Optionen für diesen Befehl:

   [-Force] [-noprompt]

Ihr Ziel ist	Dann…
Ändern Sie das Profil, um die Betriebssystemauthentifizierung zu verwenden	Geben Sie Folgendes an, anstatt den Benutzernamen, das Passwort und den Port hinzuzufügen: • -Oscaleraccount_Name als Name des Betriebssystemkontos • -Osgroupgroup als die Gruppe, die mit dem Betriebssystem-Konto verknüpft ist, in der Regel das Konto, mit dem Oracle installiert wird
Verwenden Sie die Authentifizierung der Automatic Storage Management (ASM)-Instanz, um das Profil zu erstellen	Geben Sie die Anmeldeinformationen für die Authentifizierung der ASM-Instanz an. • -Asmusernamecminstance_username ist der Benutzername, der zur Anmeldung bei der ASM-Instanz verwendet wird. • -Asmpasswordasminstance_password ist das Passwort, das zur Anmeldung bei der ASM-Instanz verwendet wird.
Verwenden Sie einen Katalog als Oracle Recovery Manager (RMAN)-Repository oder Sie möchten RMAN entfernen	Geben Sie die folgenden Optionen und Variablen an: • -Tnsname tnsname als der in der Datei nnsnames.ora definierte tnsname. • -Login -Benutzername als Benutzername, der für die Verbindung zum RMAN-Katalog erforderlich ist. Wenn nicht angegeben, verwendet SnapManager die Authentifizierungsdaten des Betriebssystems. Sie können die Betriebssystemauthentifizierung nicht mit RAC-Datenbanken (Real Application Clusters) verwenden. • -Passwordpassword als RMAN-Kennwort für die Verbindung mit dem RMAN-Katalog. • -Controlfile, wenn Sie die Steuerdatei als RMAN-Repository verwenden. • -Remove-rman um RMAN zu entfernen.

Ihr Ziel ist	Dann…
Ändern Sie die Backup Retention Policy für Backups der Datenbank im Profil	Geben Sie entweder den Aufbewahrungszeitraum oder die Aufbewahrungsdauer für eine Aufbewahrungsklasse oder beides an, um die Aufbewahrungsrichtlinie zu ändern. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). • -Hourly ist die stündliche Aufbewahrungsklasse, für die [-countn] [-durationm]]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw.. • -Daily ist die tägliche Aufbewahrungsklasse, für die [-countn] [-durationm]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw.. • -Weekly ist die wöchentliche Aufbewahrungsklasse, für die [-countn] [-durationm]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw.. • -Monthly ist die monatliche Aufbewahrungsklasse, für die [-countn] [-durationm]]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw..
Sicherer Schutz für das Profil deaktivieren	Geben Sie -noprotect an, um die mit dem Profil erstellten Datenbank-Backups nicht zu schützen. Bei einem Profil, bei dem -protect aktiviert war, wird eine Warnmeldung angezeigt, die darauf hinweist, dass dieser Vorgang den Datensatz löscht und Sie keine Backups für dieses Profil wiederherstellen oder klonen können.

Ihr Ziel ist	Dann…
E-Mail-Benachrichtigungen für den Abschlussstatus der Datenbankvorgänge aktivieren	Geben Sie die folgenden Optionen und Variablen an: • -Summary-notification ermöglicht Ihnen die Konfiguration einer E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank. • -Notification ermöglicht Ihnen, eine E-Mail-Benachrichtigung über den Status des Datenbankvorgangs für ein Profil zu erhalten. • -Success-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung nach Abschluss eines erfolgreichen Datenbankvorgangs zu erhalten, der mit einem neuen oder einem vorhandenen Profil durchgeführt wird. • -Failure-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung über einen fehlgeschlagenen Datenbankvorgang zu erhalten, der mit einem neuen oder einem vorhandenen Profil durchgeführt wird. • -Subjectsubject_Text gibt den Subjekttext für die E-Mail-Benachrichtigung an, während ein neues Profil oder ein vorhandenes Profil erstellt wird. Wenn die Benachrichtigungseinstellungen nicht für das Repository konfiguriert sind und Sie versuchen, Profile- oder Übersichtsbenachrichtigungen mithilfe der Befehlszeilenschnittstelle (CLI) zu konfigurieren, wird die folgende Meldung im Konsolenprotokoll protokolliert: SMO-14577: Benachrichtigungseinstellungen nicht konfiguriert. Wenn Sie die Benachrichtigungseinstellungen konfiguriert haben und versuchen, eine zusammenfassende Benachrichtigung mithilfe der CLI zu konfigurieren, ohne dass eine zusammenfassende Benachrichtigung für das Repository aktiviert wird, wird die folgende Meldung im Konsole-Protokoll protokolliert: SMO-14575: Konfiguration der zusammenfassenden Benachrichtigung für dieses Repository nicht verfügbar

Ihr Ziel ist	Dann…
Aktualisieren Sie das Profil, um eine Sicherung der Archiv-Log-Dateien separat zu erstellen	Geben Sie die folgenden Optionen und Variablen an: • -Separate-archivlog-Backups ermöglicht es Ihnen, eine Sicherung der Archivprotokolldateien getrennt von den Datenbankdateien zu erstellen. Nachdem Sie diese Option angegeben haben, können Sie entweder ein Datendatei-only Backup oder ein Backup nur mit Archivdateien erstellen. Sie können keine vollständige Sicherung erstellen. Außerdem können Sie die Profileinstellungen nicht durch Trennen der Sicherung zurücksetzen. SnapManager behält die Backups auf Basis der Aufbewahrungsrichtlinie für die Backups bei, die vor der Erstellung eines rein archivorientierten Backups erstellt wurden. • -Retention-archivlog-Backups legt die Aufbewahrungsdauer für Archiv-Log-Backups fest. Wenn Sie das Profil zum ersten Mal aktualisieren, können Sie die Archiv-Log-Backups vom Datendatei-Backup mit der Option -separatem-archivlog -Backups trennen; Sie müssen die Aufbewahrungsdauer für die Archiv-Log-Backups mit der Option -restyle-archivelog -Backups angeben. Die Einstellung der Aufbewahrungsdauer ist optional, wenn Sie das Profil später aktualisieren. • -Protect erstellt einen Anwendungsdatensatz im Data Fabric Manager (DFM) Server und fügt Mitglieder hinzu, die sich auf die Datenbank, Datendatei, Kontrolldateien und Archivprotokolle beziehen. Wenn der Datensatz vorhanden ist, wird er bei der Erstellung eines Profils erneut verwendet. • -Protection-Policy legt die Schutzrichtlinie auf die Archiv-Log-Backups. • -Include-with-Online-Backups geben an, dass das Archiv-Log-Backup zusammen mit dem Datenbank-Backup enthalten ist. -No-include-with-Online-Backups gibt an, dass die Sicherung der Archivprotokolldatei nicht

Ihr Ziel ist	Dann…
Ändern Sie den Hostnamen der Zieldatenbank	Geben Sie -hostNew_db_Host an, um den Hostnamen des Profils zu ändern.
Sammeln Sie die Dump-Dateien nach dem Profil-Update-Vorgang	Geben Sie die Option -dump an.

2. Geben Sie den folgenden Befehl ein, um das aktualisierte Profil anzuzeigen: `smo profile show`

Verwandte Informationen

So sammeln Sie Speicherauszugsdateien

Profile werden gelöscht

Sie können ein Profil jederzeit löschen, solange es keine erfolgreichen oder unvollständigen Backups enthält. Sie können Profile löschen, die freigegebene oder gelöschte Backups enthalten.

1. Geben Sie zum Löschen eines Profils den folgenden Befehl ein: `smo profile delete -profile profile_name`

Verwandte Informationen

Der Befehl smoprofile delete

Backup von Datenbanken

SnapManager ermöglicht das Backup von Daten auf lokalen Storage-Ressourcen mithilfe von Post-Processing-Scriptsoder durch den Schutz von Backups auf sekundären oder tertiären Storage-Ressourcen. Die Wahl zum Backup auf sekundären Storage stellt eine zusätzliche Ebene dar, die im Notfall die Daten sichert.

SnapManager ermöglicht es außerdem Storage-Administratoren, ihre Backups auf der Grundlage von Richtliniplänen zu konfigurieren. Mithilfe von SnapManager können Administratoren Backups ermitteln, die den Richtlinienanforderungen nicht entsprechen, und diese unverzüglich beheben.

SnapManager bietet folgende Optionen zum Sichern, Wiederherstellen und Wiederherstellen der Daten in Ihrer Datenbank:

- Sichern Sie die gesamte Datenbank oder einen Teil davon.

  Wenn Sie einen Teil davon sichern, geben Sie eine Gruppe von Tabellen oder eine Gruppe von Datendateien an.

- Sichern Sie die Datendateien und archivieren Sie Log-Dateien separat.
- Erstellen Sie Backups von Datenbanken auf dem primären Storage (auch als lokaler Storage bezeichnet) und sichern Sie sie durch Backups in sekundärem oder tertiärem Storage (auch Remote-Storage).
- Planen Sie routinemäßige Backups.

Wie sich SnapManager (3.2 oder höher) von früheren SnapManager Versionen unterscheidet

SnapManager (3.1 oder älter) ermöglicht Ihnen die Erstellung vollständiger Datenbank-Backups, die Datendateien, Kontrolldateien und Archivprotokolldateien enthalten.

SnapManager (3.1 oder älter) verwaltet nur die Datendateien. Die Archivprotokolldateien werden mithilfe von Lösungen außerhalb von SnapManager aufbewahrt.

SnapManager (3.1 oder früher) hat die folgenden Einschränkungen beim Management von Datenbank-Backups:

- Performance-Einbußen

  Wenn Sie ein vollständiges Online-Datenbank-Backup durchführen (wenn sich die Datenbank im Backup-Modus befindet), reduziert sich die Performance der Datenbank für den Zeitraum, bis das Backup erstellt wird. In SnapManager (ab 3.2) können begrenzte Datenbank-Backups und häufige Archiv-Log-Backups erstellt werden. Durch häufige Backups für Archivprotokolle kann verhindert werden, dass die Datenbank im Backup-Modus platziert wird.

- Manuelle Wiederherstellung und Wiederherstellung

  Wenn die erforderlichen Archivprotokolldateien nicht im aktiven Dateisystem vorhanden sind, müssen Datenbankadministratoren erkennen, welches Backup die Archivprotokolldateien enthält, die Datenbank-Backups mounten und die wiederhergestellte Datenbank wiederherstellen. Dieser Prozess ist zeitaufwändig.

- Platzbeschränkungen

  Wenn ein Datenbankbackup erstellt wird, werden die Ziele für das Archivprotokoll voll, sodass die Datenbank nicht reagiert, bis ausreichend Speicherplatz auf dem Speicher erstellt wird. In SnapManager (3.2 oder höher) können die Archiv-Log-Dateien aus dem aktiven Dateisystem heraus geschnitten werden, um regelmäßig Speicherplatz freizugeben.

Warum Archiv-Log-Backups wichtig sind

Archivprotokolldateien sind erforderlich, um die Datenbank nach einer Wiederherstellung vorwärts zu verschieben. Jede Transaktion auf einer Oracle-Datenbank wird in den Archiv-Log-Dateien erfasst (wenn sich die Datenbank im Archiv-Log-Modus befindet). Datenbankadministratoren können die Datenbank-Backups mithilfe der Archivprotokolldateien wiederherstellen.

Vorteile von nur-archivlog Backups

- Separate Aufbewahrungsdauer für nur archivlog Backups

  Es kann weniger Aufbewahrungsdauer für die rein archivbasierten Backups haben, die für die Wiederherstellung erforderlich sind.

- Schützt die nur archivorientierten Backups auf der Basis von Archivierungsprotokollschutzrichtlinien

  Sie können je nach Anforderung verschiedene Sicherungsrichtlinien für nur Archivprotokolle auswählen.

- Verbessert die Performance der Datenbank
- Konsolidiert Backups für Archivprotokolle

  SnapManager konsolidiert die Archiv-Protokoll-Backups jedes Mal, wenn Sie ein Backup erstellen, indem

die doppelten Archiv-Log-Backups freigegeben werden.

Welche SnapManager Datenbank-Backups sind

SnapManager ermöglicht Ihnen die Durchführung verschiedener Backup-Aufgaben. Sie können Aufbewahrungsklassen zuweisen, um festzulegen, wie lange das Backup aufbewahrt werden kann. Sobald diese Frist erreicht ist, wird das Backup gelöscht.

- Erstellen von Backups auf dem primären Storage
- Erstellen geschützter Backups auf den sekundären Speicherressourcen
- Überprüfen Sie, ob die Backups erfolgreich abgeschlossen wurden
- Zeigen Sie eine Liste von Backups an
- Planen Sie Backups über die grafische Benutzeroberfläche
- Verwalten Sie die Anzahl der beibehaltenen Backups
- Kostenlose Backup-Ressourcen
- Mounten und unmounten Sie Backups
- Backups löschen

SnapManager erstellt Backups mithilfe einer der folgenden Aufbewahrungsklassen:

- Stündlich
- Täglich
- Wöchentlich
- Monatlich
- Unbegrenzt

Der Protection Manager muss installiert werden, um Sicherungsrichtlinien für den Schutz von Backups zu verwenden. Ein Backup kann einen dieser Schutzzustände haben: Nicht angefordert, nicht geschützt oder geschützt.

Wenn neue Datendateien zur Datenbank hinzugefügt werden, sollten Sie sofort eine neue Sicherung erstellen. Wenn Sie außerdem ein Backup wiederherstellen, das vor dem Hinzufügen der neuen Datendateien erstellt wurde, und versuchen Sie, es nach dem Hinzufügen der neuen Datendateien zu einem Punkt wiederherzustellen, kann der automatische Recovery-Prozess fehlschlagen. Weitere Informationen zum Prozess zur Wiederherstellung der nach einem Backup hinzugefügten Datendateien finden Sie in der Oracle-Dokumentation.

Welche vollständigen und teilweisen Backups sind

Sie können die gesamte Datenbank oder nur einen Teil davon sichern. Wenn Sie einen Teil der Datenbank sichern möchten, können Sie wahlweise eine Gruppe von Tabellen oder Datendateien sichern. Sie können dabei ein separates Backup sowohl von Tabellen als auch Datendateien durchführen.

In der folgenden Tabelle sind die Vorteile und Folgen der einzelnen Backup-Typen aufgeführt:

Backup-Typ	Vorteile	Nachteile
Voll	Minimiert die Anzahl der Snapshot Kopien. Bei Online-Backups befindet sich jede Tablespace für die gesamte Zeit des Backup-Vorgangs im Backup-Modus. SnapManager erstellt für jedes Volume, das die Datenbank verwendet, eine Snapshot-Kopie sowie eine Snapshot-Kopie jedes Volumes, die sich die Protokolldateien befinden.	Bei Online-Backups befindet sich jede Tablespace für die gesamte Zeit des Backup-Vorgangs im Backup-Modus.
Teilweise	Minimiert die Zeitdauer, die jeder Tablespace im Backup-Modus verbringt. SnapManager gruppiert die von Tablespaces erstellten Snapshot Kopien. Jede Tablespace befindet sich im Backup-Modus nur lang genug, um die Snapshot-Kopien zu erstellen. Diese Methode zur Gruppierung der Snapshot Kopien minimiert die Schreibvorgänge in physischen Blöcken in Protokolldateien während eines Online-Backups.	Das Backup kann das Erstellen von Snapshot Kopien mehrerer Tabellen im selben Volume erfordern. Diese Methode kann dazu führen, dass SnapManager während des Backups mehrere Snapshot Kopien eines einzelnen Volumes erstellt.

Hinweis: Obwohl Sie eine partielle Sicherung durchführen können, müssen Sie immer eine vollständige Sicherung der gesamten Datenbank durchführen.

Backup-Typen und die Anzahl der Snapshot Kopien

Der Backup-Typ (vollständig oder teilweise) beeinflusst die Anzahl der Snapshot-Kopien, die SnapManager erstellt. Für eine vollständige Sicherung erstellt SnapManager eine Snapshot Kopie jedes Volumes, während für ein partielles Backup SnapManager eine Snapshot Kopie jeder Tablespaces-Datei erstellt.

> Data ONTAP begrenzt die maximale Anzahl an Snapshot Kopien auf 255 pro Volume. Diese maximale Anzahl erreichen Sie möglicherweise nur, wenn Sie SnapManager für eine große Anzahl von Backups konfigurieren, bei denen jedes Backup aus mehreren Snapshot Kopien besteht.

Um einen ausreichenden Backup-Pool verfügbar zu halten und gleichzeitig sicherzustellen, dass das maximale Limit von Snapshot Kopien pro Volume nicht erreicht wird, müssen Sie Backups entfernen, wenn sie nicht mehr benötigt werden. Sie können die SnapManager Aufbewahrungsrichtlinie so konfigurieren, dass erfolgreiche Backups entfernt werden, nachdem ein bestimmter Schwellenwert für eine bestimmte Backup-Frequenz erreicht wurde. Nachdem SnapManager beispielsweise vier erfolgreiche tägliche Backups erstellt hat, entfernt SnapManager die täglich erstellten Backups am Vortag.

In den folgenden Tabellen wird gezeigt, wie SnapManager Snapshot Kopien auf Grundlage des Backup-Typs erstellt. Das Beispiel in der Tabelle geht davon aus, dass Datenbank-Z zwei Volumes umfasst, jedes Volume

zwei Tabellen (TS1 und TS2) und jeder Tablespace zwei Datenbankdateien (ts1_1.dbf, ts1_2.dbf, ts2_1.dbf und ts2_2.dbf) umfasst.

In diesen Tabellen wird gezeigt, wie die beiden Backup-Typen verschiedene Anzahl von Snapshot Kopien erstellen.

SnapManager erstellt Snapshot Kopien auf Volume-Ebene anstelle von Tablespaces, die in der Regel die Anzahl der zu erstellenden Snapshot Kopien verringern.

Beide Backups erstellen auch Snapshot Kopien der Log-Dateien.

Volumes in Datenbank	Tablespace TS1 (enthält 2 Datenbankdateien)	Tablespace TS2 (enthält 2 Datenbankdateien)	Snapshot Kopien werden erstellt	Gesamtzahl der Snapshot Kopien
/Vol/Vola	TS1_1.dbf	TS2_1.dbf	1 pro Volume	2

Volumes in Datenbank	Tablespace TS1 (enthält 2 Datenbankdateien)	Tablespace TS2 (enthält 2 Datenbankdateien)	Snapshot Kopien werden erstellt	Gesamtzahl der Snapshot Kopien
/Vol/Vola	TS1_1.dbf	TS2_1.dbf	2 pro Datei	4

Vollständige Online-Backups

Während eines vollständigen Online-Backups sichert SnapManager die gesamte Datenbank und erstellt Snapshot-Kopien auf Volume-Ebene (nicht auf Ebene der Tablespaces).

SnapManager erstellt für jedes Backup zwei Snapshot-Kopien. Wenn sich alle von der Datenbank benötigten Dateien in einem einzigen Volume befinden, werden beide Snapshot-Kopien in diesem Volume angezeigt.

Wenn Sie eine vollständige Sicherung angeben, führt SnapManager die folgenden Aktionen durch:

1. Platziert die gesamte Datenbank in den Online-Backup-Modus
2. Erstellt Snapshot Kopien aller Volumes, die Datenbankdateien enthalten
3. Modus für Online-Backups wird die Datenbank aus dem Online-Backup entfernt
4. Erzwingt einen Protokollschalter und archiviert dann die Protokolldateien

   Dies überträgt auch die Redo-Informationen auf die Festplatte.

5. Generiert Backup-Kontrolldateien
6. Erstellt eine Snapshot Kopie der Log-Dateien und der Backup-Kontrolldateien

Während eines vollständigen Backups wird die gesamte Datenbank von SnapManager in den Online-Backup-Modus versetzt. Ein einzelner Tablespace (z. B. /vol/vola/ts1_1.dbf) befindet sich im Online-Backup-Modus länger als bestimmte Tabellen oder Datendateien, die angegeben wurden.

Wenn eine Datenbank in den Backup-Modus wechselt, schreibt Oracle ganze Blöcke in die Protokolle und schreibt nicht nur das Delta zwischen Backups. Da Datenbanken im Online Backup-Modus mehr Arbeit leisten,

stellt die Auswahl eines vollständigen Backups eine größere Last für den Host dar.

Obwohl die Durchführung vollständiger Backups eine größere Belastung des Hosts bewirkt, benötigen vollständige Backups weniger Snapshot-Kopien, was zu weniger Storage-Anforderungen führt.

Teilweise Online-Backups

Anstelle eines kompletten Backups können Sie wählen, ob Sie ein partielles Backup der Tabellen in einer Datenbank durchführen möchten. Während SnapManager eine Snapshot Kopie von Volumes für *Full* Backups erstellt, erstellt SnapManager für *partial* Backups eine Snapshot Kopie von jedem angegebenen Tablespace.

Da die Ebene des Tablespaces die unterste Ebene ist, die Oracle den Backup-Modus ermöglicht, verarbeitet SnapManager Backups auf Ebene des Tablespaces, auch wenn Sie eine Datendatei in einem Tablespace angeben.

Bei einem partiellen Backup ist jeder Tablespace im Backup-Modus für eine kürzere Zeit im Vergleich zu einem vollständigen Backup vorhanden. Während eines Online-Backups steht die Datenbank Benutzern jederzeit zur Verfügung. Die Datenbank muss jedoch mehr Arbeit erledigen, und der Host muss mehr physische I/O-Vorgänge durchführen Außerdem erstellt SnapManager Snapshot-Kopien von jedem angegebenen Tablespaces oder jedem Tablespace, der eine angegebene Datendatei anstelle des gesamten Volume enthält, mehr Snapshot Kopien.

SnapManager nimmt Snapshot Kopien bestimmter Tabellen oder Datendateien in Anspruch. Der partielle Backup-Algorithmus ist eine Schleife, die SnapManager wiederholt, bis eine Snapshot-Kopie von jedem angegebenen Tablespace oder einer Datendatei erstellt wurde.

> Obwohl Sie eine partielle Sicherung durchführen können, wird empfohlen, immer eine vollständige Sicherung der gesamten Datenbank durchzuführen.

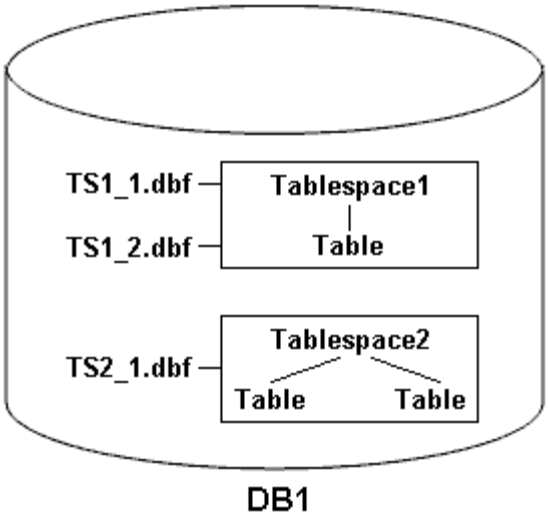
SnapManager führt während eines partiellen Backups folgende Aktionen durch:

1. Platziert den Tablespaces, der die Datendateien enthält, in den Backup-Modus.
2. Erstellt eine Snapshot-Kopie aller Volumes, die vom Tablespace verwendet werden.
3. Entfernt den Tablespace aus dem Backup-Modus.
4. Setzen Sie diesen Prozess fort, bis eine Snapshot Kopie aller Tabellen oder Dateien erstellt wurde.
5. Erzwingt einen Protokollschalter und archiviert dann die Protokolldateien.
6. Generiert Backup-Kontrolldateien
7. Erstellt eine Snapshot Kopie der Log-Dateien und der Backup-Kontrolldateien.

Beispiele für Backup-, Restore- und Recovery-Vorgänge

Hier finden Sie Informationen zu Backup-, Restore- und Recovery-Szenarien, mit denen Sie Ihre Datensicherungsziele erreichen.

In der folgenden Abbildung wird der Inhalt des Tablespaces angezeigt:



In der Abbildung hat Tablespace1 eine Tabelle und zwei Datenbankdateien mit ihr verknüpft. Tablespace2 hat zwei Tabellen und eine Datenbankdatei zugeordnet.

In der folgenden Tabelle werden einige vollständige und teilweise Backup-, Restore- und Recovery-Szenarien beschrieben:

Beispiele für vollständige Backup-, Restore- und Recovery-Vorgänge

Vollständiges Backup	Wiederherstellen	Recovery
SnapManager erstellt eine Datensicherung aller Komponenten in Datenbank DB1, einschließlich der Datendateien, Archivprotokolle und Kontrolldateien.	Vollständiges Restore mit Kontrolldateien SnapManager stellt alle Datendateien, Tablespaces und Kontrolldateien im Backup wieder her.	Sie können eine der folgenden Optionen angeben: • SCN - Geben Sie ein SCN ein, z. B. 384641. • Datum/Uhrzeit – Geben Sie ein Datum und eine Uhrzeit des Backups ein, z. B. 2005-11-25:19:06:22. • Der letzten Transaktion, die zur Datenbank durchgeführt wurde.
Vollständiges Restore ohne Kontrolldateien SnapManager stellt alle Tabellen und Datendateien ohne die Kontrolldateien wieder her.	Bei der Wiederherstellung von Datendateien oder Tablespaces mit Kontrolldateien geben Sie eine der folgenden Optionen an: • Tablespaces • Datendateien	SnapManager stellt die Daten zur letzten Transaktion wieder her, die zur Datenbank durchgeführt wurde.

Beispiele für partielle Backup-, Restore- und Recovery-Vorgänge

Teilweise Sicherung	Wiederherstellen	Recovery
Sie können eine der folgenden Optionen auswählen: • Tablespaces Sie können Tablespace1 und Tablespace2 oder nur einen von ihnen festlegen. • Datendateien Sie können alle drei Datenbankdateien (TS1_1.dbf, TS1_2.dbf und TS2_1.dbf), zwei Dateien oder eine Datei angeben. Unabhängig von der gewählten Option umfasst das Backup alle Kontrolldateien. Archivprotokolldateien sind in der Teilsicherung enthalten, wenn das Profil nicht aktiviert ist, um die Archiv-Log-Backups separat zu erstellen.	Beim Complete Restore SnapManager werden alle Datendateien, Tablespaces und Kontrolldateien, die im partiellen Backup angegeben sind, wiederhergestellt.	SnapManager stellt die Daten für die letzte Transaktion wieder her, die zur Datenbankinstanz durchgeführt wurde.

Teilweise Sicherung	Wiederherstellen	Recovery
Stellen Sie entweder Datendateien oder Tablespaces mit Kontrolldateien wieder her SnapManager führt eine der folgenden Restores durch: • Alle angegebenen Datendateien • Alle angegebenen Tablespaces	Stellen Sie entweder Datendateien oder Tablespaces ohne Kontrolldateien wieder her SnapManager führt eine der folgenden Restores durch: • Tablespaces Geben Sie einen beliebigen Tablespaces an. SnapManager stellt nur die angegebenen Tablespaces wieder her. Wenn das Backup Tablespace1 enthält, stellt SnapManager nur diese Tablespaces wieder her. • Datendateien Geben Sie eine der Datenbankdateien an. SnapManager stellt nur die angegebenen Datendateien wieder her. Wenn das Backup Datenbankdateien enthält (TS1_1.dbf und TS1_2.dbf), stellt SnapManager nur diese Dateien wieder her.	Stellen Sie nur Kontrolldateien wieder her

Über die Handhabung von Steuerdateien und Archivprotokolldateien

SnapManager enthält die Kontrolldateien und enthält optional Archivprotokolldateien für jedes Backup. Archivprotokolldateien werden für Recovery-Vorgänge verwendet.

Die Datenbank verwendet Steuerdateien, um Namen, Standorte und Größe der Datenbankdateien zu identifizieren. SnapManager umfasst in jedem Backup Kontrolldateien, da beim Restore-Prozess Kontrolldateien verwendet werden.

Die Änderungen an einer Datenbank werden mithilfe der Online-Wiederherstellungsprotokolle verfolgt, die schließlich archiviert und als archivierte Wiederherstellungsprotokolle (oder Archivprotokolle) bekannt sind. SnapManager (3.2 oder höher) ermöglicht Ihnen das separate Backup von Datendateien und die Archivierung von Protokolldateien mit verschiedenen Aufbewahrungs- und Frequenzbereichen. SnapManager kann Backups nur der Archivprotokolle oder kombinierten Backups von Datendateien und Archivprotokollen erstellen. SnapManager bietet umfassendes, automatisiertes Management von Archivprotokollen und manuelle Eingriffe in das Datenbank-Recovery und ermöglicht nach dem Backup auch die Erstellung von Archivprotokollen von einem oder mehreren Archivprotokollzielen.

Um anzuzeigen, welche Tabellen und Datendateien in ein Backup enthalten sind, verwenden Sie den Befehl Backup show oder das Fenster Backup Properties.

Die folgende Tabelle zeigt, wie SnapManager Protokolldateien während jeder Ausführung und Archivierung

verarbeitet:

[OPTIONS=„Header“]d

Art des Vorgangs	Kontrolldateien	Archivierung von Protokolldateien
Backup	Bei jedem Backup enthalten	Kann bei jedem Backup berücksichtigt werden
Wiederherstellen	Sowohl allein als auch zusammen mit den Tabellen oder Datendateien können wiederhergestellt werden	Kann für den Wiederherstellungsprozess verwendet werden

Was ist für ein Datenbank-Backup geplant

Sie können Backups für Datenbanken mithilfe der Registerkarte Zeitplan der grafischen Benutzeroberfläche planen, aktualisieren und überwachen.

Die folgende Tabelle behandelt einige häufig gestellte Fragen zur Zeitplanung:

Frage	**Antwort**
Was geschieht mit den geplanten Backups, wenn der SnapManager Server neu gestartet wird?	Beim Neustart des SnapManager-Servers werden alle Zeitpläne automatisch neu gestartet. SnapManager wird jedoch nicht zu verpassten Vorkommnissen nachgehen.

Frage	Antwort
Was geschieht, wenn zwei Backups gleichzeitig auf zwei Datenbanken geplant werden?	SnapManager startet die Backup-Vorgänge nacheinander und ermöglicht es dann, die Backups parallel auszuführen. Wenn ein Datenbankadministrator beispielsweise sechs tägliche Backup-Pläne für sechs verschiedene Datenbankprofile erstellt, die um 1:00 Uhr stattfinden, werden alle sechs Backups parallel ausgeführt. Wenn für einen kurzen Zeitraum mehrere Backups auf einem einzelnen Datenbankprofil geplant werden, führt der SnapManager-Server nur den Backup-Vorgang mit der längsten Aufbewahrungsdauer aus. Vor dem Starten eines Backup-Vorgangs legt SnapManager zunächst Folgendes fest: • Hat ein anderer Zeitplan in den letzten 30 Minuten erfolgreich ein Backup mit größerer Aufbewahrung für dasselbe Profil erstellt? • Wird ein anderer Zeitplan innerhalb der nächsten 30 Minuten versuchen, ein Backup mit größerer Aufbewahrung für dasselbe Profil zu erstellen? Wenn die Antwort auf eine der Fragen „Ja“ lautet, wird das Backup von SnapManager übersprungen. Beispielsweise kann ein Datenbankadministrator einen täglichen, wöchentlichen und monatlichen Zeitplan für ein Datenbankprofil erstellen, der alle Backups um 1:00 Uhr vorbestimmt sind An diesem Tag des Monats, an dem drei Backups gleichzeitig um 1:00 Uhr stattfinden sollen, führt SnapManager nur den Backup-Vorgang aus, der auf dem monatlichen Zeitplan basiert. Das Zeitfenster von 30 Minuten kann in einer SnapManager-Eigenschaftendatei geändert werden.
Unter welchem Benutzer wird die Sicherung ausgeführt?	Der Vorgang wird unter dem Benutzer ausgeführt, der den Zeitplan erstellt hat. Sie können dies jedoch in Ihre eigene Benutzer-ID ändern, wenn Sie sowohl für das Datenbankprofil als auch für den Host gültige Anmeldeinformationen haben. Durch das Starten von geplanten Backup-Eigenschaften für den von Avida Davis erstellten Backup-Zeitplan kann Stella Morrow beispielsweise seine Benutzer-ID für diesen Vorgang als Benutzer auswählen, um das geplante Backup auszuführen.

Frage	Antwort
Wie funktioniert der SnapManager Scheduler mit dem systemeigenen Scheduler?	Auf dem SnapManager-Server können Sie die geplanten Backups nicht über den systemeigenen Scheduler des Betriebssystems anzeigen. Zum Beispiel, nach dem Erstellen eines geplanten Backups, sehen Sie keine zusätzlichen Einträge in cron.

Frage	Antwort
Was passiert, wenn die Uhren in der grafischen Benutzeroberfläche und der Server nicht synchronisiert sind?	Die Uhren auf Client und Server werden nicht synchronisiert. So können Sie ein Backup planen, bei dem sich die Startzeit künftig auf dem Client, aber in der Vergangenheit auf dem Server befindet. Bei wiederkehrenden Backups erfüllt der Server die Anforderung immer noch. Wenn der Server beispielsweise eine Anfrage erhält, stündliche Backups ab dem 01/30/08 um 3:00 Uhr durchzuführen Aber die aktuelle Zeit ist 3:30 Uhr An diesem Tag führt der Server sein erstes Backup um 4:00 Uhr durch Und führt weiterhin Backups jede Stunde durch. Für einmalige Backups übernimmt der Server jedoch die Anfrage wie folgt: • Wenn sich die Startzeit innerhalb der letzten fünf Minuten nach der aktuellen Serverzeit befindet, beginnt SnapManager sofort mit dem Backup. • Wenn die Startzeit größer als fünf Minuten ist, startet SnapManager das Backup nicht. Betrachten wir zum Beispiel das folgende Szenario: • Die Uhr im Host der grafischen Schnittstelle liegt drei Minuten hinter der eigentlichen Zeit. • Die aktuelle Zeit auf dem Client ist 8:58 Uhr • Sie planen, ein einmalig auszusichertes Backup um 9:00 Uhr zu erstellen • Sie planen ein weiteres, einmalig zu besichertes Backup um 8:30 Uhr Wenn der Server die erste Anforderung erhält, ist die Uhrzeit auf dem Server 9:01 Uhr Obwohl sich die Startzeit für das Backup in der Vergangenheit befindet, führt SnapManager sofort das Backup durch. Wenn der Server die zweite Anforderung erhält, beträgt der Startzeit des Backups mehr als fünf Minuten in der Vergangenheit. Sie erhalten eine Meldung, dass die Terminanfrage fehlgeschlagen ist, da die Startzeit in der Vergangenheit liegt. Sie können die Zeit von fünf Minuten in einer SnapManager-Eigenschaftendatei ändern.

Frage	Antwort
Was geschieht mit den geplanten Backups für ein Profil, wenn das Profil gelöscht wird?	Wenn ein Datenbankprofil gelöscht wird, löscht der SnapManager-Server geplante Backups, die für dieses Profil definiert wurden.
Wie verhalten sich geplante Backups während der Sommerzeit oder bei einer Änderung der SnapManager Serverzeit?	SnapManager Backup-Zeitpläne sind aufgrund der Sommerzeit oder beim Ändern der SnapManager Server-Zeit betroffen. Berücksichtigen Sie bei einer Änderung der Uhrzeit des SnapManager-Servers folgende Auswirkungen: • Nachdem der Backup-Zeitplan ausgelöst wurde, falls der SnapManager Server wieder zurückfällt, wird der Backup-Zeitplan nicht wieder ausgelöst. • Wenn die Sommerzeit vor der geplanten Startzeit beginnt, werden die Backup-Pläne automatisch ausgelöst. • Wenn Sie sich zum Beispiel in den USA befinden, planen Sie stündliche Backups um 4:00 Uhr Dies sollte alle 4 Stunden stattfinden. Backups werden um 4 Uhr, 8 Uhr, 12 Uhr, 4 Uhr, 8 Uhr und Mitternacht an den Tagen vor und nach der Sommerzeit im März und November durchgeführt. • Beachten Sie Folgendes, wenn die Backups für 2:30 Uhr geplant sind Jede Nacht: ◦ Wenn die Uhren eine Stunde zurückfallen, da das Backup bereits ausgelöst wurde, wird das Backup nicht erneut ausgelöst. ◦ Wenn die Uhren eine Stunde vorwärts springen, löst das Backup sofort aus. Wenn Sie sich in den USA befinden und dieses Problem vermeiden möchten, müssen Sie Ihre Backups so planen, dass sie außerhalb von 2:00 Uhr beginnen Bis 3:00 Uhr Intervall:

Datenbank-Backups werden erstellt

Backups von ganzen Datenbanken oder Teilen von Datenbanken, einschließlich Tabellen, Datendateien oder Kontrolldateien, können erstellt werden.

SnapManager bietet Snapshot-Kopien für Datenbanken in vielen Host-seitigen Storage-Stacks, einschließlich NFS, ASM, Veritas und anderen.

Bei RAC-Konfigurationen (Real Application Clusters) führt SnapManager die Sicherung auf Hostseite im Profil durch.

Administratoren können optional Backups mit Oracle RMAN registrieren, um die Datenbank mit granulareren Besonderheiten wie Blöcken wiederherzustellen.

Sie können die Namen der Snapshot Kopien, die durch Backups dieses Profils erstellt werden, während Sie dieses Profil definieren. Beispielsweise können Sie eine Präfixzeichenfolge mit HOPS einfügen, um High Operations Backups zu kennzeichnen.

Sie können nicht nur eindeutige Namen für Snapshot Kopien definieren, die durch Backups erstellt werden, sondern auch eindeutige Bezeichnungen für die Backups selbst erstellen. Wenn Sie ein Backup erstellen, ist es eine gute Praxis, einen Namen für das Backup anzugeben, so dass Sie eine einfache Möglichkeit haben, es mit dem Parameter -Label zu identifizieren. Dieser Name muss für alle Backups, die innerhalb eines bestimmten Profils erstellt wurden, eindeutig sein. Der Name kann Buchstaben, Zahlen, Unterstrich (_) und Bindestrich (-) enthalten. Es kann nicht mit einem Bindestrich beginnen. Bei Etiketten wird die Groß-/Kleinschreibung beachtet. Möglicherweise möchten Sie Informationen wie Umgebungsvariablen des Betriebssystems, Systemdatum und Backup-Typ anhängen.

Wenn Sie kein Etikett bereitstellen, erstellt SnapManager im Formular scope_Mode_datestring einen Standardnamen mit dem Namen scope_Mode_datestring, wobei der Umfang voll oder teilweise ist und der Modus offline, online oder automatisch ist (der Buchstabe c für kalt, h für heiß oder A für automatisch).

Ab SnapManager 3.4 können Sie Ihr eigenes Backup-Label bereitstellen, indem Sie das von SnapManager erstellte Standard-Backup-Label überschreiben. Sie müssen den Wert des Parameters override.default.backup.pattern auf true setzen und im Parameter new.default.backup.pattern die neue Sicherungsbezeichnung angeben. Das Backup-Label-Muster kann Schlüsselwörter wie Datenbankname, Profilname, Umfang, Modus und Hostname enthalten, die durch Unterstrich getrennt werden müssen. Beispiel: new.default.backup.pattern=dbname_profile_hostname_scope_mode.

Der Zeitstempel wird automatisch am Ende des generierten Etiketts eingefügt.

Wenn Sie einen Kommentar eingeben, können Sie Leerzeichen und Sonderzeichen enthalten. Wenn Sie hingegen ein Etikett eingeben, enthalten Sie keine Leerzeichen oder Sonderzeichen.

Für jedes Backup generiert SnapManager automatisch eine GUID, eine 32-stellige HEX-Zeichenfolge. Zum Bestimmen der GUID müssen Sie den Befehl für die Sicherungsliste mit der Option -wortrecih ausführen.

Sie können eine vollständige Sicherung einer Datenbank erstellen, während diese online oder offline ist. Um SnapManager mit der Sicherung einer Datenbank umgehen zu lassen, unabhängig davon, ob sie online oder offline ist, sollten Sie die Option -Auto verwenden.

Wenn Sie beim Erstellen eines Backups die Beschneidung aktiviert haben und die zusammenfassende Benachrichtigung im Profil aktiviert wurde, werden zwei separate E-Mails ausgelöst. Eine E-Mail ist für den Backup-Vorgang und die andere für die Beschneidung. Sie können diese E-Mails korrelieren, indem Sie den Backup-Namen und die Backup-ID in diesen E-Mails vergleichen.

Sie können ein Cold Backup erstellen, wenn sich die Datenbank im Shutdown-Status befindet. Wenn sich die Datenbank in einem gemounteten Zustand befindet, ändern Sie sie in einen Shutdown-Status, und führen Sie das Offline-Backup (Cold Backup) durch.

Mit SnapManager (3.2 oder höher) können Sie die Archivprotokolldateien getrennt von den Datendateien sichern und so die Archivprotokolldateien effizient verwalten.

Um die Backups des Archivprotokolls separat zu erstellen, müssen Sie ein neues Profil erstellen oder das bestehende Profil aktualisieren, um die Backup des Archivprotokolls mit der Option -separatem-archivlog -Backups zu trennen. Mithilfe des Profils können Sie die folgenden SnapManager-Vorgänge durchführen:

- Erstellen Sie eine Backup-Datei für Archivprotokolle.
- Löschen Sie eine Sicherung des Archivprotokolls.

- Mounten Sie ein Backup für das Archivprotokoll.
- Kostenlose Backup eines Archivprotokolls.

Die Backup-Optionen variieren je nach Profileinstellungen:

- Mit einem Profil, das nicht getrennt ist, um Archiv-Log-Backups separat durchzuführen, können Sie Folgendes tun:
  - Erstellen Sie ein vollständiges Backup.
  - Erstellen Sie ein partielles Backup.
  - Geben Sie für Archivprotokolldateien zu sichernde Ziele an.
  - Geben Sie Archivprotokollziele an, die vom Backup ausgeschlossen werden sollen.
  - Legen Sie die Beschneiungsoptionen für das Löschen der Archivprotokolldateien aus den Archivprotokollzielen fest.
- Mithilfe eines Profils, das zur Erstellung von Archiv-Log-Backups getrennt ist, können Sie Folgendes tun:
  - Erstellen Sie ein Backup nur für Datendateien.
  - Erstellen Sie ein Backup nur archivels.
  - Während Sie ein Backup nur für Datendateien erstellen, schließen Sie das Backup des Archivprotokolls zusammen mit den online gespeicherten Datendateien nur zum Klonen ein.

    Wenn Sie Archiv-Log-Backups zusammen mit Datendateien auf der Seite **Profileinstellungen** des Assistenten **Profile Create** der SnapManager-Benutzeroberfläche enthalten haben, Und wenn Sie die Option **Archivierungsprognogs** im Assistenten * Backup Create* nicht ausgewählt haben, erstellt SnapManager immer das Archiv-Log Backup zusammen mit Datendateien für alle Online-Backups.

    In einer solchen Situation können Sie über die SnapManager-CLI alle Ziele für das Archiv-Protokoll für die Sicherung außer den in der SnapManager-Konfigurationsdatei angegebenen Ausschlusszielen betrachten. Aber Sie können diese Archiv-Log-Dateien nicht beschneiden. Allerdings können Sie immer noch die Option -archivoogs verwenden, um das Ziel der Archivprotokolldatei anzugeben und die Archivprotokolldateien von der SnapManager CLI zu beschneiden.

    Wenn Sie die Datensicherung mit der Option -Auto erstellen und die Option --archivprotokolle angeben, erstellt SnapManager entweder ein Online- oder Offline-Backup auf Grundlage des aktuellen Status des Backups.

    - SnapManager erstellt ein Offline Backup, wenn die Datenbank offline ist und keine Archivprotokolldateien in das Backup berücksichtigt.
    - SnapManager erstellt ein Online Backup einschließlich Archiv-Log-Dateien, wenn die Datenbank online ist.
  - Während das nur Archivprotokolle erstellt wird:
    - Geben Sie das Archivprotokoll-Ziel an, das gesichert werden soll, zusammen mit dem nur-Archivprotokoll-Backup
    - Geben Sie die Ziele für das Archivprotokoll an, die vom Backup nur für Archivprotokolle ausgeschlossen werden sollen
    - Legen Sie die Beschneiungsoptionen für das Löschen der Archivprotokolldateien aus den Archivprotokollzielen fest
- **Szenarien nicht unterstützt**
  - Sie können das nur-Archivprotokoll-Backup nicht zusammen mit einem Offline-Datendatei-Backup

erstellen.

- Sie können die Archivprotokolldateien nicht beschneiden, wenn die Archivprotokolldateien nicht gesichert sind.
- Sie können die Archivprotokolldateien nicht beschneiden, wenn der Flash Recovery Area (FRA) für Archivprotokolldateien aktiviert ist.

  Wenn Sie im Bereich Flash Recovery den Speicherort für das Archivprotokoll angeben, müssen Sie im Parameter Archive_log_dest auch den Speicherort für das Archivprotokoll angeben.

Wenn Sie das Label für die Sicherung von Online-Datendateien mit dem enthaltenen Archiv-Log-Backup angeben, wird das Etikett für die Datensicherung von Datendateien angewendet, und das Archiv-Log-Backup wird mit (_logs) aufgestickt. Dieses Suffix kann konfiguriert werden, indem der Parameter Suffix.Backup.Label.with.logs in der SnapManager-Konfigurationsdatei geändert wird.

Sie können beispielsweise den Wert als Suffix.Backup.Label.with.logs=Arc angeben, sodass der Standardwert _logs in _Arc geändert wird.

Wenn Sie keine Ziele für das Archivprotokoll angegeben haben, die in das Backup aufgenommen werden sollen, enthält SnapManager alle in der Datenbank konfigurierten Archivprotokollziele.

Wenn in einem der Ziele keine Archivprotokolldateien fehlen, überspringt SnapManager alle diese Archivprotokolldateien, die vor den fehlenden Archivprotokolldateien erstellt wurden, selbst wenn diese Dateien in anderen Archivprotokollzielen verfügbar sind.

Während der Erstellung von Archiv-Log-Backups müssen Sie die Ziele für die Archivprotokolldatei angeben, die in die Sicherung aufgenommen werden sollen, und können den Konfigurationsparameter so einstellen, dass die Archivprotokolldateien immer über die fehlenden Dateien in der Sicherung hinausgehen.

Standardmäßig ist dieser Konfigurationsparameter auf true gesetzt, um alle Archivprotokolldateien über fehlende Dateien hinaus einzubeziehen. Wenn Sie Ihre eigenen Archiv-Log-Beschneidungsskripte verwenden oder Archivprotokolldateien manuell aus den Archiv-Protokollzielen löschen, können Sie diesen Parameter deaktivieren, damit SnapManager die Archivprotokolldateien überspringen und weiter mit der Sicherung fortfahren kann.

SnapManager unterstützt die folgenden SnapManager Vorgänge für Backups des Archivprotokolls nicht:

- Klonen der Backup des Archivprotokolls
- Backup des Archivprotokolls wiederherstellen
- Backup des Archivprotokolls überprüfen

SnapManager unterstützt auch die Sicherung der Archivprotokolldateien aus den Zielen des Flash-Recovery-Bereichs.

1. Geben Sie den folgenden Befehl ein: bbs Backup create -profile_Name {[-full {-online} -offline} [-contake {-hourly — Weekly { -unlimited}] [-verify] [-dataces [[-filesfiles [files] [-Tabellen-Tabellen [-Tabellen]] [-datalabellabel] {-online [-offline-} [-contake-monthly-commocellabel] [-snapvaultlabelSnapVault_Label][-Protect [-noprotect] [-Backup-destpath1 [,[path2]]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all -untilSCN-bis-dato yyyy-MM-dd:HH:mm:s -destune-wours] [{}}}-defune-months]

Ihr Ziel ist	Dann…
Erstellen Sie mithilfe der *SnapManager_cDOT_Vault* Schutzrichtlinie ein Backup auf sekundärem Storage	Geben Sie -snapvaultltlLabel an. Sie müssen das SnapMirror-Label bereitstellen, das Sie in den Regeln der SnapMirror-Richtlinie angegeben haben, und gleichzeitig die SnapVault-Beziehung als Wert einrichten.
Geben Sie an, ob Sie eine Sicherung einer Online- oder Offline-Datenbank durchführen möchten, anstatt SnapManager zu erlauben, ob es online oder offline ist	Geben Sie -offline an, um eine Sicherung der Offline-Datenbank zu erstellen. Geben Sie -online an, um eine Sicherung der Online-Datenbank durchzuführen. + Wenn Sie diese Optionen verwenden, können Sie die Option -Auto nicht verwenden.
Geben Sie an, ob SnapManager die Sicherung einer Datenbank handhaben soll, unabhängig davon, ob sie online oder offline ist	Geben Sie die Option -Auto an. Wenn Sie diese Option verwenden, können Sie die Option --offline oder -online nicht verwenden.

Geben Sie an, ob Sie eine partielle Sicherung bestimmter Dateien durchführen möchten	`Specify the -data-files option and then list the files, separated by commas. For example, list the file names f1, f2, and f3 after the option.`
	`+ Beispiel für die Erstellung einer partiellen Datendatei-Sicherung auf UNIX`
	
	+
	
	`smo backup create -profile nosep -data -files /user/user.dbf -online -label partial_datafile_backup -verbose`

Ihr Ziel ist	Dann…
Geben Sie an, ob Sie eine partielle Sicherung bestimmter Tabellen durchführen möchten	``` Specify the -data-tablespaces option and then list the tablespaces, separated by commas. For example, use ts1, ts2, and ts3 after the option. + SnapManager unterstützt das Backup von schreibgeschützten Tablespaces. Beim Erstellen des Backups ändert SnapManager die schreibgeschützten Tabellenbereiche zu lesen/schreiben. Nach dem Erstellen des Backups werden die Tabellen auf schreibgeschützt geändert. ``` + Beispiel zum Erstellen einer Datensicherung für Teiltablespaces + ``` smo backup create -profile nosep -data -tablespaces tb2 -online -label partial_tablespace_bkup -verbose ```
Geben Sie an, ob Sie für jedes Backup ein eindeutiges Label im folgenden Format erstellen möchten: Full_Hot_mybackup_Label	``` For Linux, you might enter this example: ``` + ``` smo backup create -profile targetdb1_prof1 -label full_hot_my_backup_label -online -full -verbose ```

Ihr Ziel ist	Dann…
Geben Sie an, ob Sie eine Sicherungskopie der Archivprotokolldateien getrennt von den Datendateien erstellen möchten	``` Specify the following options and variables: ** -Archivalogs erstellt eine Sicherung der Archiv-Log-Dateien. ** -Backup-dest gibt die Ziele für die Archivprotokolldatei an, die gesichert werden sollen. ** -Exclude-dest gibt die zu ausgeschlossenen Archivprotokollziele an. ** -Label gibt die Bezeichnung für die Sicherung der Archivprotokolldatei an. ** -Protect bietet Schutz für die Archiv-Log-Backups. *Hinweis:* Sie müssen entweder die Option -Backup-dest oder die Option -exclude-dest angeben. ``` + Wenn Sie beide Optionen zusammen mit der Fehlermeldung „Backup zeigt“ angeben, haben Sie eine ungültige Backup-Option angegeben. Geben Sie eine der Optionen an: -Backup-dest oder exclude-dest. + Beispiel für die Erstellung von Backups von Archivprotokolldateien getrennt auf UNIX + ``` smo backup create -profile nosep -archivelogs -backup-dest /mnt/archive_dest_2/ -label archivelog_bkup -verbose ```

Ihr Ziel ist	Dann…
Geben Sie an, ob Sie eine Datensicherung der Datendateien erstellen und Protokolldateien archivieren möchten	``` Specify the following options and variables: ** -Data Option, um die Datendateien anzugeben. ** -Archivalogs Option zur Angabe der Archiv-Log-Dateien. Beispiel für das Sichern von Datendateien und Archivprotokolldateien zusammen auf UNIX ``` + ``` smo backup create -profile nosep -data -online -archivelogs -backup-dest mnt/archive_dest_2 -label data_arch_backup -verbose ```

Ihr Ziel ist	Dann…
Geben Sie an, ob Sie die Archiv-Log-Dateien beim Erstellen eines Backups beschneiden möchten	``` Specify the following options and variables: ** -Prunelogs gibt an, die Archiv-Log-Dateien aus den Archiv-Log-Zielen zu löschen. ``` + *** -All gibt an, alle Archiv-Log-Dateien aus den Archiv-Log-Zielen zu löschen.** * -Bis-scntabis-scn gibt an, die Archivprotokolldateien bis zu einem angegebenen SCN zu löschen. *** -Until-dateyyyyy -MM-dd:HH:mm:ss gibt an, die Archiv-Log-Dateien bis zum angegebenen Zeitraum zu löschen.** * -Before gibt an, die Archivprotokolldateien vor dem angegebenen Zeitraum zu löschen (Tage, Monate, Wochen, Stunden). ***** -Prune-destprune_dest1,[prune_dest2 gibt an, die Archiv-Log-Dateien aus den Archiv-Protokollzielen zu löschen, während die Sicherung erstellt wird. **Hinweis:** die Archivprotokolldateien können nicht beschnitten werden, wenn der Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist. + Beispiel für das Beschneiden aller Archiv-Log-Dateien während der Erstellung einer Sicherung auf UNIX + + + ``` smo backup create -profile nosep -archivelogs -label archive_prunebackup1 -backup-dest /mnt/arc_1,/mnt/arc_2 -prunelogs -all -prune-dest /mnt/arc_1,/mnt/arc_2 -verbose ```
Geben Sie an, ob Sie einen Kommentar zum Backup hinzufügen möchten	„Specify -comment“ gefolgt von der Beschreibungstext.

Ihr Ziel ist	Dann…
Geben Sie an, ob Sie die Datenbank in den Zustand zwingen möchten, den Sie angegeben haben, um sie zu sichern, unabhängig davon, in welchem Zustand sie sich derzeit in befindet	Geben Sie die Option -Force an.
Geben Sie an, ob Sie das Backup gleichzeitig überprüfen möchten, wenn Sie es erstellen	Geben Sie die Option -verify an.
Geben Sie an, ob Sie die Dump-Dateien nach dem Datenbank-Backup-Vorgang sammeln möchten	Geben Sie die -dump-Option am Ende des Befehls zum Erstellen von Backups an.

Beispiel

```
smo backup create -profile targetdb1_prof1 -full -online -force  -verify
```

Verwandte Informationen

Benennen von Snapshot-Kopien

Erstellen von vor-, Post-Task- und Richtlinienskripten

Aufgabenskripte werden erstellt

Speichern der Taskskripte

Der Befehl smo Backup erstellen

Sicherung von Datenbank-Backups auf sekundärem oder tertiärem Storage

Beschneiden von Archivprotokolldateien

Sie können die Archiv-Log-Dateien aus den Archiv-Log-Speicherorten beschneiden, während Sie eine Sicherung erstellen.

- Archivprotokolldateien müssen durch den aktuellen Backup-Vorgang gesichert werden.

  Wenn der Beschnitt zusammen mit anderen Backups angegeben wird, die keine Archivprotokolldateien enthalten, werden die Archivprotokolldateien nicht beschnitten.

- Die Datenbank muss sich im angehängten Status befinden.

  Wenn die Datenbank nicht angehängt ist, geben Sie die Option -Force zusammen mit dem Backup-Befehl ein.

Während eines Backup-Vorgangs können Sie Folgendes angeben:

- Beschnitt:

- Löschen Sie alle Archivprotokolldateien.
- Löschen Sie die Archivprotokolldateien bis zur angegebenen Systemänderungsnummer (SCN).
- Löschen Sie die Archivprotokolldateien bis zum angegebenen Zeitpunkt.
- Löschen Sie die Archivprotokolldateien vor dem angegebenen Zeitraum.

- Ziel, von dem die Archivprotokolldateien beschnitten werden müssen.

Selbst wenn die Archivprotokolldatei Beschnitt in einem Ziel fehlschlägt, beschnitten SnapManager weiterhin die Archivprotokolldateien von den anderen Zielen.

Vor dem Löschen der Archivprotokolldateien überprüft SnapManager Folgendes:

- Archivprotokolldateien werden mindestens einmal gesichert.
- Archivprotokolldateien werden, falls vorhanden, an die Oracle Dataguard Standby-Datenbank gesendet.
- Archivprotokolldateien werden, falls vorhanden, durch den Oracle Stream-Erfassungsprozess erfasst.

Wenn die Archivprotokolldateien gesichert, in den Standby-Modus versetzt und vom Erfassungsprozess erfasst werden, löscht SnapManager alle Archivprotokolldateien in einer einzigen Ausführung. Wenn es jedoch Archivprotokolldateien gibt, die nicht gesichert, nicht in den Standby-Modus geliefert oder nicht durch den Erfassungsprozess erfasst werden, löscht SnapManager die Archivprotokolldateien nacheinander. Das Löschen von Archivprotokollen-Dateien in einer einzigen Ausführung ist schneller als das Löschen von Archivprotokollen.

SnapManager kann auch die Archivprotokolldateien gruppieren und Batch-by-Batch löschen. Jeder Batch hat maximal 998 Dateien. Dieser Wert kann unter 998 mit dem Konfigurationsparameter Maximum.archivelog.files.toprune.atATIME in der Datei smo.config konfiguriert werden.

SnapManager verwendet zum Löschen der Archivprotokolldateien den Befehl Oracle Recovery Manager (RMAN). SnapManager ist jedoch nicht mit den RMAN Aufbewahrungsrichtlinien und Löschrichtlinien integriert.

Wenn Sie die Archivprotokolldateien aus den Archivprotokollzielen löschen, schlägt das Beschneiden von Archivprotokolldateien fehl.

SnapManager unterstützt das Beschneiden von Archiv-Log-Dateien in den folgenden Szenarien nicht:

- Im Bereich Flash Recovery befinden sich Archivprotokolldateien.
- Archivprotokolldateien befinden sich in der Standby-Datenbank.
- Die Archivprotokolldateien werden sowohl von SnapManager als auch von RMAN gemanagt.

  a. Geben Sie den folgenden Befehl ein: bbs Backup create -profile_Name {[-full {-online { -offline} [-contake {-hourly [-Daily { -Weekly} -unlimited}] [-confirm] [-dataces [-monthly-commentaces [-monthly-contaces] [-monthly-commoceptaces [-monthly}] [-monthly-commoceptaces [-monthly] [-monthly-loceptaces] [-] [-monthly-monthly] [-monthly-loceptaces [-] [-monthly-lo [-protect [-protect-protect] [,[path2]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all - untilSCN -bis-dateyyyyyy-MM-dd:HH:mm:ss [-estune-spunefficile-prune-je[{}}}-destune-jew]

Ihr Ziel ist	Dann…
Prune Archivprotokolldateien	Legen Sie die folgenden Optionen fest: • -Prunelogs gibt an, die Archivprotokolldateien beim Erstellen einer Sicherung zu löschen. ◦ -All gibt an, alle Archiv-Log-Dateien zu löschen. ◦ -UntilSCN gibt an, die Archivprotokolldateien bis zum angegebenen SCN zu löschen. ◦ -Bis-date gibt an, dass die Archivprotokolle gelöscht werden, einschließlich des angegebenen Datums und der angegebenen Uhrzeit. ◦ -Vor {-Monaten
-Tage	-Wochen
-Hours} gibt an, dass die Archiv-Log-Dateien vor dem angegebenen Zeitraum gelöscht werden.	**Das Ziel, aus dem die Archiv-Log-Dateien beschnitten werden sollen**, sollte einbezogen werden

Konsolidierung von Backups für Archivprotokolle

SnapManager konsolidiert die nur-Archivierten Backups jedes Mal, wenn Sie ein Backup erstellen, indem die doppelten, nur-Archivierten Backups freigesetzt werden. Standardmäßig ist Konsolidierung aktiviert.

SnapManager erkennt die nur archivlog Backups, die in anderen Backups Archivprotokolle haben und gibt ihnen die Möglichkeit, eine Mindestanzahl an nur Archivprotokoll-Dateien aufrechtzuerhalten.

Wenn die nur Archivprotokolle durch Konsolidierung freigegeben werden, dann werden diese Backups basierend auf der Aufbewahrungsdauer des Archivprotokolls gelöscht.

Wenn sich die Datenbank während der Konsolidierung des Archivprotokolls im Shutdown- oder Nomount-Status befindet, ändert SnapManager die Datenbank in den Bereitstellungsstatus.

Wenn die Sicherung oder Beschneidung von Archiv-Log-Dateien fehlschlägt, dann wird die Konsolidierung nicht durchgeführt. Die Konsolidierung von nur-archivlog Backups wird nur nach erfolgreichen Backups und erfolgreichen Anstiftungen verfolgt.

1. Um die Konsolidierung der nur archivlog Backups zu ermöglichen, ändern Sie die Konfigurationsparameter-Konsolidierung und setzen Sie den Wert in der SnapManager Konfigurationsdatei (smo.config) als wahr ein.

   Sobald der Parameter festgelegt ist, werden die archivlog-only Backups konsolidiert.

   Wenn das neu erstellte Archivprotokoll-only Backup die gleichen Archivprotokolldateien in einem der früheren nur-Archivprotokolle enthält, dann werden die Backups des früheren Archivprotokolls freigegeben.

SnapManager konsolidiert nicht das Backup des Archivprotokolls, das zusammen mit dem Datendateien-Backup aufgenommen wurde. SnapManager konsolidiert das nur archivBackup.

SnapManager konsolidiert die Archiv-Log-Backups selbst dann, wenn der Benutzer die Archiv-Log-Dateien manuell aus den Archiv-Log-Zielen löscht oder wenn die Archiv-Log-Dateien beschädigt sind und möglicherweise die Sicherung enthalten.

2. Um die Konsolidierung der Archiv-Log-Backups zu deaktivieren, ändern Sie die Konfigurationsparameter-Konsolidierung und setzen Sie den Wert in der SnapManager-Konfigurationsdatei (smo.config) als false.

Planung der Beschneidung der Archivprotokolldatei

Wenn Sie ein Backup erstellen, können Sie die Beschneidung von Archivprotokolldateien für eine bestimmte Zeit planen.

Mit SnapManager können Sie die Archivprotokolldateien regelmäßig aus dem aktiven Dateisystem beschneiden.

1. Geben Sie den folgenden Befehl ein: `smo schedule create -profile profile_name {[-full {-online | -offline | -auto}[-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]] | [-data [-filesfiles [files]] | [-tablespaces-tablespaces [-tablespaces]] {-online | -offline | -auto}[-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]] | [-archivelogs]} [-commentcomment] [-protect | -protectnow | -noprotect] [-backup-destpath1 [,[path2]] [-exclude-destpath1 [,path2]] [-prunelogs{-all | -untilSCNuntilSCN | -before {-dateyyyy-MM-dd HH:mm:ss | -monthsmonths | -weeksweeks | -daysdays | -hourshours}} -prune-destprune_dest1,,prune_dest2] -schedule -nameschedule_name [-schedule-commentschedule_comment] -interval {-hourly | -daily | -weekly | -monthly | -onetimeonly} -cronstringcronstring-start-time {start-timestart_time <yyyy-MM-dd HH:mm>} -runasuser-runasuser [-force] [-quiet | -verbose]`

Ihr Ziel ist	Dann…
Planen eines Beschneidung von Archivprotokolldateien	Legen Sie die folgenden Optionen fest: • -Prunelogs zu planen Beschneidung der Archiv-Log-Dateien • -Prune-dest Archivprotokolldateien aus den Archivprotokollzielen zu prune
• Einen Namen für den Terminplan angeben*	Geben Sie die Option -terminplan-Name an.

Ihr Ziel ist	Dann…
Planen Sie das Beschneiden von Archivprotokolldateien in einem bestimmten Zeitintervall	Geben Sie die Intervalloption an und geben Sie an, ob die Archivprotokolldateien auf der Grundlage der folgenden Intervallklassen beschnitten werden sollen: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • Nur -ontimeonly
Fügen Sie einen Kommentar über die Terminplanoperation	Geben Sie die Option -terminieren-comment an, gefolgt von der Beschreibungszeichenfolge.
Geben Sie die Startzeit der Zeitplanoperation an	Geben Sie die Option -Start-time im Format yyyy-mm-dd hh:mm an.

Sicherung von Backups für Archivprotokolle

Während der Erstellung von Profilen können Sie den Schutz für die Backups des Archivprotokolls basierend auf der Schutzrichtlinie für Archivprotokolle aktivieren.

1. Geben Sie den folgenden Befehl ein: `smo profile create -profileprofile [-profile-passwordprofile_password] -repository-dbnamerepo_dbname-hostrepo_host -portrepo_port-login-usernamerepo_username-database-dbnamedb_dbname -hostdb_host [-siddb_sid] [-login-usernamedb_username-passworddb_password-portdb_port] [-rman {-controlfile | {-login-usernamerman_username-passwordrman_password-tnsnamerman_tnsname} }] -osaccountosaccount -osgrouposgroup [-retain [-hourly [-countn] [-durationm]] [-daily [-countn] [-durationm]] [-weekly [-countn] [-durationm]] [-monthly [-countn] [-durationm]]] [-commentcomment][-snapname-patternpattern][-protect [-protection-policypolicy_name]] [-summary-notification] [-notification [-success-emailemail_address1, email_address2-subjectsubject_pattern] [-failure-emailemail_address1, email_address2-subjectsubject_pattern]][-separate-archivelog-backups-retain-archivelog-backups-hourshours | -daysdays | -weeksweeks| -monthsmonths [-protect [-protection-policypolicy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]`

Wenn…	Dann…
Sie wollen Archiv-Log-Backups separat sichern und die Archiv-Log-Dateien schützen	Legen Sie die folgenden Optionen fest: • -Separatem-archivlog-Backups ermöglicht es Ihnen, die Archiv-Log-Dateien von den Datendateien zu trennen. • -Protect weist eine separate Schutzrichtlinie für die Archiv-Log-Backups des Archivprotokolls zu. • -Protection-Policy weist die Schutzrichtlinie für die Archiv-Log-Backups zu.

Was ist AutoSupport

Die AutoSupport-Funktion ermöglicht es dem SnapManager Server, nach Abschluss des Backup-Vorgangs AutoSupport Meldungen an das Storage-System zu senden.

SnapManager sendet AutoSupport-Meldungen nur für erfolgreiche Backup-Vorgänge.

Sie können AutoSupport aktivieren oder deaktivieren, indem Sie dem Konfigurationsparameter Auto_Support.on in der Konfigurationsdatei smo.config die folgenden Werte zuweisen:

- TRUE – aktiviert AutoSupport
- FALSE - deaktiviert AutoSupport

Standardmäßig ist AutoSupport in SnapManager aktiviert.

Verwandte Informationen

Hinzufügen von Storage-Systemen, die in Clustered Data ONTAP betrieben werden, zum SnapManager Server-Host

Aktivierung von AutoSupport in SnapManager

Deaktivieren von AutoSupport in SnapManager

Hinzufügen von Storage-Systemen, die in Clustered Data ONTAP betrieben werden, zum SnapManager Server-Host

Sie müssen die Storage-Systeme, die in Clustered Data ONTAP ausgeführt werden, zum SnapManager Server Host hinzufügen, um AutoSupport zu aktivieren. Ab SnapManager 3.3 wurde AutoSupport nur auf Storage-Systemen mit 7-Mode unterstützt.

1. Ergänzen Sie den SnapManager Server-Host um Storage-Systeme, die in Clustered Data ONTAP betrieben werden.

Wenn…	Führen Sie dann den folgenden Befehl aus…
Admin Storage Virtual Machine (SVM, ehemals bekannt als Vserver) wird in Clustered Data ONTAP ausgeführt	SnapDrive config set -cserver user_nameStorage_Name
SVM wird in Clustered Data ONTAP betrieben	SnapDrive config set -vServer user_nameStorage_Name

Aktivierung von AutoSupport in SnapManager

Sie müssen AutoSupport aktivieren, damit Storage-Systeme bei jedem erfolgreichen Backup-Vorgang Meldungen vom SnapManager-Server empfangen.

AutoSupport kann auf zwei Arten aktiviert werden:

- Standardmäßig enthält die neue Installation von SnapManager nicht den Parameter Auto_Support.on in der Konfigurationsdatei smo.config. Dies impliziert, dass AutoSupport aktiviert ist.
- Sie können den Parameter Auto_Support.on manuell konfigurieren.
  a. Beenden Sie den SnapManager-Server.
  b. Legen Sie in der Konfigurationsdatei smo.config den Wert des Parameters Auto_Support.on auf TRUE fest.

     auto_Support.on=TRUE

  c. Starten Sie den SnapManager-Server neu.

Deaktivieren von AutoSupport in SnapManager

Sie müssen AutoSupport deaktivieren, wenn das Storage-System bei jedem erfolgreichen Backup-Vorgang keine Meldungen vom SnapManager-Server empfangen soll.

Standardmäßig ist AutoSupport aktiviert, wenn die Konfigurationsdatei den Parameter Auto_Support.on nicht enthält. In diesem Szenario müssen Sie den Parameter Auto_Support.on in der Konfigurationsdatei hinzufügen und den Wert AUF FALSE setzen.

1. Beenden Sie den SnapManager-Server.
2. Legen Sie in der Konfigurationsdatei smo.config den Wert für den Parameter Auto_Support.on auf FALSE fest.

   auto_Support.on=FALSE

3. Starten Sie den SnapManager-Server neu.

Datenbank-Backups werden überprüft

Sie können mit dem Befehl Backup Verify überprüfen, ob die Blöcke im Datenbank-Backup nicht beschädigt sind. Der Verify-Vorgang ruft das Dienstprogramm Oracle

Database Verify für jede Datendatei im Backup auf.

Mit SnapManager können Sie den Verifizierungsvorgang jederzeit für Sie und die Benutzer in Ihrem System durchführen. Sie können die Verifizierung sofort nach dem Erstellen des Backups durchführen. Sie müssen das Profil angeben, das das Backup enthält, und entweder die Bezeichnung oder die ID des erstellten Backups.

Sie können -dump angeben, um die Dump-Dateien nach der Backup-Überprüfung zu sammeln.

1. Geben Sie den folgenden Befehl ein: `smo backup verify -profile profile_name [-label label | -idid] [-force] [ -dump] [-quiet | -verbose]`

Verwandte Informationen

Der Befehl smo Backup verify

Ändern der Richtlinie zur Aufbewahrung von Backups

Sie können die Eigenschaften eines Backups ändern, sodass dieser gemäß der Aufbewahrungsrichtlinie zum Löschen berechtigt oder nicht zur Verfügung steht.

Wenn Sie ein Backup erstellen, können Sie dessen Aufbewahrungsrichtlinie festlegen. Sie können später wählen, ob Sie das Backup für einen längeren Zeitraum aufbewahren möchten, als die Aufbewahrungsrichtlinie es zulässt oder angeben, dass Sie das Backup nicht mehr benötigen und die Aufbewahrungsrichtlinie es verwalten soll.

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Dauerhaft Aufbewahrung von Backups

Sie können angeben, dass ein Backup durch die Aufbewahrungsrichtlinie nicht zur Löschung berechtigt sein sollte, um das Backup auf unbestimmte Zeit zu halten.

1. Geben Sie den folgenden Befehl ein, um anzugeben, dass ein Backup unbegrenzt aufbewahrt werden soll: `smo backup update -profileprofile_name {-labellabel [data | -archivelogs] | -idid} -retain -unlimited`

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Zuweisen von Backups mit einer bestimmten Aufbewahrungsklasse

Datenbankadministratoren können Backups mit einer bestimmten Aufbewahrungsklasse stündlich, täglich, wöchentlich oder monatlich durchführen. Durch das Zuweisen einer bestimmten Aufbewahrungsklasse können die unter dieser Änderung durchgeführten Backups gelöscht werden.

1. Um eine bestimmte Backup-Aufbewahrungs-Klasse zuzuweisen, geben Sie diesen Befehl ein:smo Backup Update -profilprofile_Name {-labellabel [Data} -archivelogs]

Ändern des Standardverhaltens der Aufbewahrungsrichtlinie

Wenn ein Backup basierend auf der Aufbewahrungsrichtlinie abläuft, bestimmt SnapManager basierend auf den Aufbewahrungseinstellungen, ob das Backup gelöscht werden soll. Das Löschen von Backups ist das Standardverhalten. Sie können dieses Standardverhalten ändern und stattdessen die ungeschützten Backups freigeben.

Standardmäßig löscht SnapManager Backups, je nachdem, ob sie wie folgt geschützt sind oder nicht:

- Für geschützte Backups entlastet SnapManager die lokalen Backups, sobald diese ablaufen.
- Bei ungesicherten Backups löscht SnapManager die lokalen Backups nach ihrem Ablauf.

  Sie können dieses Standardverhalten ändern.

Bei geschützten Backups berücksichtigt SnapManager nicht die folgenden Kriterien bei der Bestimmung, ob die lokale Kopie gelöscht werden soll:

- Das Backup auf den sekundären Storage ist ausgefallen oder wird gerade geschützt.

  Dies ermöglicht die Übertragung von Backups auf den Sekundärspeicher, bevor die Aufbewahrungsrichtlinie angewendet wird.

- Die Kopie wurde anschließend aus dem Sekundärspeicher gelöscht.
  a. Zugriff auf den folgenden Standardspeicherort:

     Standard smo Installationsort/Properties/smo.config

  b. Bearbeiten Sie die Datei smo.config.
  c. Legen Sie in der Datei smo.config die Eigenschaft contee.alwayFreeExpiredBackups auf true fest.

     Beispiel: „Exkepe.alwayFreeExpiredBackups“ = „true“

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Freistellen oder Löschen von Backups ohne Rücknahmerichtlinien

Backups mit einer „unbegrenzten“ Aufbewahrungsklasse können nicht direkt gelöscht oder freigegeben werden. Um diese Backups zu löschen oder zu löschen, müssen Sie zunächst eine andere Aufbewahrungsklasse wie stündlich, täglich, wöchentlich oder monatlich zuweisen. Um ein Backup zu löschen oder zu befreien, das von der Aufbewahrungsrichtlinie ausgenommen ist, müssen Sie zuerst das Backup aktualisieren, um es für die Löschung berechtigt zu machen oder es freizumachen.

1. Um das Backup zu aktualisieren, damit es durch die Aufbewahrungsrichtlinie zum Löschen berechtigt ist, geben Sie den folgenden Befehl ein: `smo backup update -profileprofile_name {-labellabel [data | -archivelogs] | -idid} -retain [-hourly | -daily | -weekly | -monthly]`
2. Nachdem Sie die Sicherung aktualisiert haben, damit sie gelöscht werden kann, können Sie entweder das Backup löschen oder kostenlose Backup-Ressourcen.

- Um das Backup zu löschen, geben Sie folgenden Befehl ein: smo Backup delete -profilprofile_Name {-labellabel [Data} -archivelogs] - idid - all
- Um die Backup-Ressourcen freizumachen, anstatt das Backup zu löschen, geben Sie diesen Befehl ein:smo Backup free -profileprofile_Name {-labellabel [Data} -archivelogs] [-did [-all [-Force] [-dump] [-quiet

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Anzeigen einer Liste von Backups

Sie können überprüfen, welche Backups für ein Profil und den Backup-Status erstellt wurden, indem Sie den Befehl smo Backup list verwenden. Der Befehl zeigt für jedes Profil zuerst die Informationen zum letzten Backup an und fährt dann fort, bis die Informationen für alle Backups angezeigt werden.

1. Geben Sie den folgenden Befehl ein: `smo backup list -profileprofile_name [-delimitercharacter] [data | -archivelogs] [-quiet | -verbose]`

Verwandte Informationen

Der Befehl smo Backup list

Anzeigen von Backup-Details

Sie können die detaillierten Informationen über ein bestimmtes Backup in einem Profil mit dem smo Backup show Befehl anzeigen.

Mit dem smo Backup show-Befehl werden die folgenden Informationen für jedes Backup angezeigt:

- Die Backup-ID
- Ob die Sicherung erfolgreich war oder fehlgeschlagen ist
- Backup-Umfang (vollständig, teilweise, online oder offline)
- Backup-Modus
- Mount-Status
- Das Backup-Etikett
- Kommentar
- Das Datum und die Uhrzeit, zu der der Vorgang gestartet und beendet wurde
- Informationen darüber, ob das Backup verifiziert wurde
- Die Kategorie für die Aufbewahrung von Backups
- Die Datenbank und der Hostname
- Die Kontrollpunkt-Systemänderungsnummer (SCN)
- Das Ende-Backup-SCN (nur für Online-Backups)
- Die Tabellen und Datendateien der gesicherten Datenbank
- Die Kontrolldateien aus der Datenbank gesichert

- Die Archivprotokolle aus der gesicherten Datenbank
- Das Storage-System und die Volumes, auf denen sich die Dateien befinden
- Die erstellten Snapshot Kopien und deren Speicherort
- Der Status der primären Storage-Ressourcen
- Der Sicherungsstatus
- Eine Liste der Kopien auf dem sekundären Speicher in Form von Backup_copy ID - Node Name
- Backup-Modus

Wenn Sie die Option -wortrecih angeben, werden die folgenden zusätzlichen Informationen angezeigt:

- Die Klone, die aus dem Backup erstellt werden, sofern vorhanden sind
- Verifizierungsinformationen
- Wenn das Backup gemountet ist, zeigt SnapManager die verwendeten Mount-Punkte an

Für die Sicherung der Archivprotokolldatei werden dieselben Informationen angezeigt wie die der anderen Datenbanksicherung, mit Ausnahme der folgenden Informationen:

- Checkpoint SCN
- Backup-SCN beenden
- Tablespace
- Kontrolldateien

Die Sicherung der Archivprotokolldatei enthält jedoch die folgenden zusätzlichen Informationen:

- Die erste Änderungsnummer des Backups
- Die nächste Nummer des Backups
- Thread-Nummer
- Protokoll-ID zurücksetzen
- Inkarnation
- Name der Protokolldatei

a. Geben Sie den folgenden Befehl ein: `smo backup show -profileprofile_name {-labellabel [data | -archivelogs] | -id id [-quiet | -verbose]`

Verwandte Informationen

Der Befehl smo Backup show

Montage von Backups

SnapManager übernimmt automatisch das Mounten eines Backups, um es dem Host zur Verfügung zu stellen. Sie können Backups auch in Szenarien einbinden, in denen Sie ein externes Tool wie Oracle Recovery Manager (RMAN) für den Zugriff auf die Dateien im Backup verwenden.

Wenn Sie RMAN verwenden, müssen Sie den Mount-Vorgang verwenden, um den Status eines Backups zu ändern (wodurch der Zugriff möglich ist) und den Unmount-Vorgang, um den Status eines Backups zu ändern

(wodurch der Zugriff entfernt wird).

Der Befehl smo Backup Mount zeigt eine Liste von Pfaden an, wo die Snapshot Kopien, die aus dem Backup bestehen, gemountet wurden.

Sie können die Option -from-secondary verwenden, um das Backup aus dem sekundären Speicher zu mounten. Wenn Sie diese Option nicht verwenden, hängt SnapManager das Backup vom primären Storage ab.

Sie müssen die Option -copy-id angeben, wenn Sie die Option -from-secondary angeben. Wenn auf dem sekundären Speichersystem mehrere Backups vorhanden sind, wird mit der Option -copy-id angegeben, welche Sicherungskopie auf dem sekundären Speicher zum Mounten des Backups verwendet werden soll.6

> Wenn Sie Data ONTAP in 7-Mode verwenden, müssen Sie einen gültigen Wert für die Option -copy-id angeben. Wenn Sie jedoch Clustered Data ONTAP verwenden, ist die Option -copy-id nicht erforderlich.

Wenn Sie ein Datenbank-Backup auf einen Remote-Host mounten, müssen Sie sicherstellen, dass die ASM-Anmeldedaten auf beiden Hosts dieselben sind.

> Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Backup-Mount-Vorgang sammeln.

1. Geben Sie zum Mounten eines Backups den folgenden Befehl ein: `smo backup mount -profile profile_name {labellabel [data | -archivelogs] | -idid} [-host-host] [-from-secondary [-copy-id id]] [-dump] [-quiet | -verbose]`

Verwandte Informationen

Der Befehl smo Backup Mount

UnMounten von Backups

SnapManager hängt automatisch das Backup ab, damit es nicht auf dem Host-Server verfügbar ist. Mit SnapManager können Sie auch die Einbindung aufheben, wenn Sie ein externes Tool wie beispielsweise den Oracle Recovery Manager (RMAN) verwenden, um auf die Dateien im Backup zuzugreifen und den Zustand des Backups zu ändern, um den Zugriff zu entfernen.

Wenn Sie die Installation eines Datenbank-Backups von einem Remote-Host aufheben, müssen Sie sicherstellen, dass die ASM-Anmeldedaten auf beiden Hosts identisch sind.

Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Unmount-Backup sammeln.

Der Unmount Vorgang kann irgendwann mit einer Fehlermeldung fehlschlagen, wenn der Mount-Punkt beschäftigt ist, z. B. --[ERROR] FLOW-11019: Fehler in Disconnect: SD-10046: Sie können das Backup nicht unmounten, da der Mount-Punkt mit den folgenden Mount-Pfaden und PIDs belegt ist: /Opt/NetApp/smo/mnt/-mnt-nebuse_nfsvrdb_ARCH-20120427052319903_0 mit PID 6598.

Sie müssen die PID der Sitzung identifizieren, die zum Ausfall des unmounten-Vorgangs führt. Beenden Sie die Sitzung, indem Sie den folgenden Befehl ausführen: `kill pid`

Anschließend können Sie die Unmount-Operation erfolgreich ausführen.

1. Geben Sie den folgenden Befehl ein: `smo backup unmount -profile profile_name {labellabel [data | -archivelogs] | -idid} [-quiet | -verbose] -dump-force -verbose`

Verwandte Informationen

Der Befehl smo Backup unmount

So werden Backups entlastet

Sie können Backups freigeben, die die Snapshot Kopien löschen, ohne die Backup-Metadaten zu löschen. Diese Funktion gibt den Speicherplatz frei, der durch das Backup belegt wird. Sie können den Smo-Backup-freien Befehl verwenden, um die Backups zu befreien.

Damit ein Backup zur Freigabe berechtigt ist, müssen Sie Folgendes sicherstellen:

- Das Backup war erfolgreich
- Backup soll nicht angehängt werden
- Backup verfügt nicht über Klone
- Der Backup darf nicht durch eine Richtlinie zur unbegrenzten Aufbewahrung beibehalten werden
- Das Backup wird nicht bereits freigegeben

Wenn die Sicherung im Profil aktiviert wird und die Sicherungsrichtlinie Verbindungen vom primären Node enthält, die eine Spiegelbeziehung verwenden, werden Snapshot-Kopien auf dem primären Node gelöscht, wenn ein Backup freigegeben wird. Diese Snapshot-Kopien werden auch bei der nächsten Übertragung zum sekundären Storage von den Spiegelknoten gelöscht.

Wenn Sie ein geschütztes Backup freigeben, fordert SnapManager an, dass Protection Manager die lokalen Snapshot-Kopien für das Backup entfernt. Wenn der freie Backup-Vorgang für die geschützten Backups erfolgreich ist, werden die Snapshot Kopien asynchron durch den Protection Manager gelöscht.

Sicherungsstatus	Lokaler Status	Aktion für den Primär-Storage	Aktion auf dem sekundären Storage	Erklärung
Nicht angefordert (zu schützen)	Vorhanden	Nimmt das Backup frei	Keine Aktion erforderlich	SnapManager befreit das lokale Backup.
Freigegeben	Keine Aktion erforderlich	Keine Aktion erforderlich	Das lokale Backup wird bereits freigegeben.	Nicht geschützt

Sicherungsstatus	Lokaler Status	Aktion für den Primär-Storage	Aktion auf dem sekundären Storage	Erklärung
Vorhanden	Nimmt das Backup frei	Keine Aktion erforderlich	SnapManager befreit das lokale Backup, auch wenn im sekundären Storage keine Kopien vorhanden sind.	Freigegeben
Keine Aktion erforderlich	Keine Aktion erforderlich	Das lokale Backup wird bereits freigegeben.	Geschützt	Vorhanden
Nimmt das Backup frei	Keine Aktion erforderlich; das Backup auf dem Sekundärsystem bleibt erhalten	SnapManager befreit das lokale Backup. Kopien verbleiben auf dem sekundären Storage.	Freigegeben	Keine Aktion erforderlich

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen freien Backup-Vorgang zu sammeln.

1. Geben Sie folgenden Befehl ein: smo Backup free -profilprofile_Name {-labellabel [Data} -archivelogs] [-quiet] [-Force]

Verwandte Informationen

Der smo Backup kostenlose Befehl

Backups werden gelöscht

Sie müssen Backups löschen, wenn Sie sie nicht mehr benötigen. Dadurch wird der Speicherplatz frei, den diese Backups belegen. Wenn Sie Backups entfernen, reduzieren Sie die Wahrscheinlichkeit, dass pro Volume 255 Snapshot Kopien erreicht werden.

- Sie müssen sicherstellen, dass das Backup nicht zum Erstellen eines Klons verwendet wurde.

Wenn Sie ein geschütztes Backup löschen, löscht SnapManager das Backup aus dem sekundären Storage und dem SnapManager Repository. Die folgende Tabelle zeigt die Aktionen, die beim Löschen eines lokalen Backups sowohl für den primären als auch für den sekundären Storage durchgeführt wurden:

Sicherungsstatus	Lokaler Status	Aktion für den Primär-Storage	Aktion auf dem sekundären Storage	Erklärung
Nicht angefordert (zu schützen)	Vorhanden	Löscht die Snapshot Kopien	Keine Aktion erforderlich	SnapManager löscht das lokale Backup.

Sicherungsstatus	Lokaler Status	Aktion für den Primär-Storage	Aktion auf dem sekundären Storage	Erklärung
Freigegeben	Keine Aktion erforderlich	Keine Aktion erforderlich	Das lokale Backup wird bereits freigegeben. Wenn Sie ein freizugebenden Backup löschen, werden die Backup-Metadaten aus dem Repository entfernt.	Nicht geschützt
Vorhanden	Löscht die Snapshot Kopien	Keine Aktion erforderlich	SnapManager löscht das lokale Backup unabhängig davon, ob das Backup geschützt ist.	Freigegeben
Keine Aktion erforderlich	Keine Aktion erforderlich	Das lokale Backup wird bereits freigegeben. Wenn Sie ein freizugebenden Backup löschen, werden die Backup-Metadaten aus dem Repository entfernt.	Geschützt	Vorhanden
Löscht die Snapshot Kopien	SnapManager löscht das Backup im sekundären Storage	SnapManager löscht das lokale Backup und die sekundären Kopien.	Freigegeben	Keine Aktion erforderlich

Wenn Sie versuchen, ein Backup zu löschen, das durch sekundären Storage geschützt ist, werden die Snapshot Kopien möglicherweise zum Löschen markiert und später durch Protection Manager gelöscht.

Sie können Backups, die unbegrenzt aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Optional können Sie die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen Backup-Löschvorgang sammeln.

Wenn Sie die Backups des Archivprotokolls löschen möchten, müssen Sie die für die Sicherung des Archivprotokolls festgelegte Aufbewahrungsdauer überprüfen. Wenn das Backup des Archivprotokolls innerhalb der Aufbewahrungsdauer liegt und die Archivprotokolldateien für die Wiederherstellung einer wiederhergestellten Datenbank erforderlich sind, können Sie das Backup des Archivprotokolls nicht löschen.

1. Überprüfen Sie, ob die Vorgänge abgeschlossen sind, indem Sie den folgenden Befehl eingeben: smo Operationliste -profilprofile_Name-quiet-wortrecih
2. Um ein Backup zu löschen, geben Sie den folgenden Befehl ein:smo Backup delete -profile profile profile Profile_Name [-Label Label [Data - archivalogs] [-idid [-Force] [-dump] [-quiet

Verwenden Sie die Option -Force, um das Entfernen des Backups zu erzwingen. Wenn Sie das Entfernen eines Backups erzwingen, bei dem unvollständige Vorgänge ausgeführt werden, ist das Backup möglicherweise inkonsistent.

Planen von Datenbank-Backups

Mit SnapManager (3.2 oder höher) für Oracle können Sie Datenbank-Backups regelmäßig während der Stoßzeiten planen, um eine hohe Performance zu gewährleisten. Zum Planen eines Backups können Sie ein Profil erstellen, das die Datenbankinformationen und die Aufbewahrungsrichtlinie enthält, und anschließend die Zeitpläne für das Backup festlegen.

Sie müssen die Backups entweder als Root-Benutzer oder als Oracle-Benutzer planen. Wenn Sie versuchen, die Backups als nicht vorhandener Benutzer zu planen, zeigt SnapManager eine Fehlermeldung an: Ungültiger Benutzer: Benutzername: Kann keinen Zeitplan-Backup für einen bestimmten Benutzer erstellen

Im Folgenden sind einige planungsbezogene Aufgaben aufgeführt:

- Planen Sie ein Datenbank-Backup auf Stundenbasis, täglich, wöchentlich, monatlich oder einmalig.
- Anzeigen einer Liste geplanter Backups, die einem Profil zugeordnet sind.
- Aktualisierung eines geplanten Backups.
- Einen Zeitplan vorübergehend aussetzen.
- Setzen Sie den angehängten Zeitplan fort.
- Löschen Sie einen Zeitplan.

Das Kontrollkästchen **Jetzt-Menü-Betrieb ausführen** ist deaktiviert, wenn eine geplante Sicherung für diesen Zeitplan ausgeführt wird.

Erstellen von Backup-Zeitplänen

Sie können ein Backup so planen, dass es zu der Zeit und Häufigkeit erfolgt, die für Ihre Daten und Ihre Umgebung geeignet sind.

Ab SnapManager 3.2 für Oracle können Sie die Backups der Archivprotokolldateien separat planen. Sie müssen jedoch das Profil verwenden, das Sie erstellt haben, um die Archivprotokolldateien zu trennen.

Wenn Sie die Backups der Datendateien und Archivprotokolldateien gleichzeitig geplant haben, erstellt SnapManager zuerst die Datensicherung.

Wenn Sie das Planungsintervall nur als -onetimeonly auswählen, stehen alle Beschneidungsoptionen zur Verfügung. Wenn Sie ein anderes Intervall als nur -onetimeonly auswählen, werden die Beschneidungsoptionen -bis-SCN und -bis-date nicht unterstützt und die folgende Fehlermeldung angezeigt: Die von Ihnen angegebene Option Archivprotokoll pruning, -bis-scn oder -bis-date für das Stundenplanintervall ist ungültig. Geben Sie entweder die Option -ontimeonly für das Planintervall an, oder beschneiden Sie die Archivprotokolle mit einer der Optionen all oder -before {-months} -days/ -weeks -hours.

Wenn in einer HACMP-Umgebung (High Availability Cluster Multiprocessing) ein Failover stattfindet, müssen

Sie den SnapManager für Oracle Server neu starten, damit die Service-Adresse (virtuelle) dem aktiven Host zugeordnet wird und die SnapManager-Zeitpläne auf den aktiven SnapManager Host angepasst werden. Diese Informationen können Sie in den HACMP-Failover-Skripten für die Vorverarbeitung oder Nachbearbeitung hinzufügen.

Wenn in einem anderen Repository derselbe Profil- und Planungsname vorhanden ist, wird der Backup-Planungsvorgang in diesem Repository nicht gestartet. Der Vorgang wird mit der folgenden Meldung beendet: Der Vorgang wird bereits ausgeführt.

1. Geben Sie den folgenden Befehl ein: bbs Schedule create -profile_Name {[-full {-online { -offline}[-contake [-hourly — Weekly — unlimited] [-verify] [-datasten [-data-dataecaces [files] [-online [-offline} [-contake [-monthly-commenttognaces] [-monthly-contake [-monthly-contaces] [-}] [-monthly-contake [- -Noprotect] [-Backup-destpath1 [,[path2]] [-exclude-destpath1 [,path2]] [-prunelogs{-all { -untilSCN -until-dateyyyyyy-MM-dd HH:mm:ss [-prune-destraune-time] [-runyyyyytime-term-term-date-time] [}} {} {<}]

Ihr Ziel ist	Dann…
Planen Sie eine Sicherung einer Online- oder Offline-Datenbank	Geben Sie -offline oder -online an, um ein Backup der Offline- oder Online-Datenbank zu planen. Wenn Sie diese angeben, können Sie nicht -Auto verwenden.
Lassen Sie SnapManager die Planung einer Datenbank handhaben, unabhängig davon, ob sie online oder offline ist	Angabe -Auto. Wenn Sie „-Auto“ angeben, können Sie „--offline“ oder „-online“ nicht verwenden.
Planen Sie eine Sicherung von Datendateien	Geben Sie -Data -files an, um die durch Kommas getrennten Dateien aufzulisten. Verwenden Sie zum Beispiel die Dateinamen f1,f2,f3.
Planen Sie eine partielle Sicherung bestimmter Tabellen	Legen Sie -Tablespaces fest, um die durch Kommas getrennten Tablespaces aufzulisten. Verwenden Sie zum Beispiel ts1,ts2,ts3.
Planen der Sicherung von Archiv-Log-Dateien	Geben Sie Folgendes an: • -Archivalogs, um die Sicherung der Archivprotokolldateien zu planen • -Backup-dest, um die Ziele für die Archivprotokolldatei zu planen, die in die Sicherung aufgenommen werden sollen • -Exclude-dest, um die Ziele für das Archivprotokoll zu planen, die vom Backup ausgeschlossen werden sollen

Ihr Ziel ist	Dann…
Geben Sie die Werte der Aufbewahrungsklasse an	Geben Sie -Retention an und geben Sie an, ob das Backup gemäß einer der folgenden Aufbewahrungsklassen aufbewahrt werden soll: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • -Unbegrenzte SnapManager standardmäßig auf stündlich.
Planen eines Beschneidung von Archivprotokolldateien	Geben Sie Folgendes an: **-Prunelogs, um die Archivprotokolldateien während der Planung eines Backups zu beschneiden** -prune-dest, um das Archivprotokollziel anzugeben, von dem die Archivprotokolldateien beschnitten werden
• Einen Namen für den Terminplan angeben*	Geben Sie -Schedule-Name an.
Sicherung der Datenbank in einem bestimmten Zeitintervall planen	Geben Sie die Option Intervall an und wählen Sie das Zeitintervall aus der folgenden, mit dem die Backups erstellt werden sollen: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • Nur -ontimeonly

Ihr Ziel ist	Dann…
Konfigurieren Sie einen Zeitplan	Geben Sie -cronstring an und enthalten die folgenden sieben Unterausdrücke, die die einzelne Option beschreiben: • 1 bezieht sich auf Sekunden. • 2 bezieht sich auf Minuten. • 3 bezieht sich auf Stunden. • 4 bezieht sich auf einen Tag im Monat. • 5 bezieht sich auf den Monat. • 6 bezieht sich auf einen Tag in einer Woche. • (Optional) 7 bezieht sich auf das Jahr. **Hinweis:** Wenn Sie Ihre Sicherung mit verschiedenen Zeiten in -cronstring und -Start-time geplant haben, dann wird der Zeitplan der Sicherung überschrieben und durch die -Start-Time ausgelöst.
Fügen Sie einen Kommentar zum Backup-Zeitplan	„Specify -terminist-comment“ gefolgt von der Beschreibungstext.
Geben Sie die Startzeit der Zeitplanoperation an	Geben Sie die Startzeit im Format yyyy-mm-dd hh:mm an.
Ändern Sie den Benutzer des geplanten Backup-Vorgangs während der Planung des Backups	Geben Sie -runasuser an. Der Vorgang wird ausgeführt als Benutzer (Root-Benutzer oder Oracle-Benutzer), der den Zeitplan erstellt hat. Sie können jedoch Ihre eigene Benutzer-ID verwenden, wenn Sie gültige Anmeldeinformationen sowohl für das Datenbankprofil als auch für den Host haben.
Aktivieren Sie eine Voraufgabe oder Nachaufgabe des Backup-Zeitplanvorgangs, indem Sie die XML-Datei mit der XML-Datei für die vor- und Nachaufgabe verwenden	Geben Sie die Option -taskSpec an und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation für die Durchführung einer Vorverarbeitung oder einer Nachbearbeitung an, die vor oder nach dem Backup-Zeitplan stattfinden soll.

Aktualisieren eines Backup-Zeitplans

Sie können eine Liste geplanter Vorgänge anzeigen und gegebenenfalls aktualisieren. Sie können die Planungsfrequenz, die Startzeit des Zeitplans, den cronstring-Ausdruck und den Benutzer, der das Backup geplant hat, aktualisieren.

1. Geben Sie folgenden Befehl ein, um den Zeitplan für ein Backup zu aktualisieren: `smo schedule update -profile profile_name-schedule-nameschedulename [-schedule-commentschedule comment] -interval {-hourly | -daily | -weekly | -monthly |`

```
-onetimeonly} -start-timestarttime-cronstringcronstring-runasuserrunasuser [-
quiet | -verbose]
```

Anzeigen einer Liste geplanter Vorgänge

Sie können eine Liste der geplanten Vorgänge für ein Profil anzeigen.

1. Um Informationen über den geplanten Vorgang anzuzeigen, geben Sie den folgenden Befehl ein: `smo schedule list -profile profile_name[-quiet | -verbose]`

Anhalten von Backup-Zeitplänen

SnapManager ermöglicht Ihnen die Unterbrechung eines Backup-Zeitplans, bis der Backup-Zeitplan wiederaufgenommen wird.

Sie können die aktiven Zeitpläne unterbrechen. Wenn Sie versuchen, den bereits unterbrochenen Backup-Zeitplan zu unterbrechen, wird möglicherweise die Fehlermeldung „Schedule <planename> bereits im Status „suspendieren“ angezeigt.

1. Um den Backup-Zeitplan vorübergehend zu unterbrechen, geben Sie folgenden Befehl ein: `smo schedule suspend -profile profile_name-schedule-nameschedulename [-quiet | -verbose]`

Wiederaufnahme der Backup-Pläne

Administratoren haben die Möglichkeit, den angehängten Backup-Zeitplan fortzusetzen.

Wenn Sie versuchen, die aktiven Zeitpläne wieder aufzunehmen, wird möglicherweise die Fehlermeldung „kann nicht fortgesetzt werden: Zeitplan <planename> bereits im Status „fortsetzen“ angezeigt.

1. Um den suspendierten Backup-Zeitplan fortzusetzen, geben Sie diesen Befehl ein: smo Schedule resume -profile Profile_Name-Schedule-nameschedulename [-quiet / -verbose]

Löschen von Backup-Zeitplänen

Sie können Backup-Pläne löschen, wenn diese nicht mehr benötigt werden.

1. Um den Backup-Zeitplan zu löschen, geben Sie folgenden Befehl ein: smo Schedule delete -profile profile_Name-Schedule-nameschedulename [-quiet - verbose]

Datenbank-Backups werden wiederhergestellt

Mit SnapManager für Oracle können Sie eine Datenbank in den Zustand wiederherstellen, an dem sie zum Zeitpunkt der Erstellung einer Snapshot Kopie erstellt wurde. Zusätzlich zum dateibasierten Restore-Prozess unterstützt SnapManager Volume-basierte Technologien zur schnellen Wiederherstellung, was die Restore-Zeit im Vergleich zu anderen Recovery-Methoden deutlich verkürzt. Da Backups häufiger erstellt werden, verringert sich die Anzahl der anzuwendenden Protokolle, sodass die mittlere Zeit bis zur Recovery (MTTR) für eine Datenbank reduziert wird.

Im Folgenden werden einige Aufgaben aufgeführt, die Sie im Zusammenhang mit dem Wiederherstellen und Wiederherstellen von Daten in Datenbanken ausführen können:

- Durchführung einer dateibasierten Wiederherstellung oder einer Volume-basierten Wiederherstellung – die schnellste Methode zur Wiederherstellung von Datenbank-Backups und die von SnapManager verwendete Standardeinstellung
- Stellen Sie das gesamte Backup oder einen Teil des Backups wieder her.

  Wenn Sie einen Teil davon wiederherstellen, geben Sie eine Gruppe von Tabellen oder eine Gruppe von Datendateien an. Sie können auch die Kontrolldateien zusammen mit den Daten oder nur die Kontrolldateien selbst wiederherstellen.

- Stellen Sie die Daten entweder nach einem bestimmten Zeitpunkt oder auf allen verfügbaren Protokollen wieder her, in denen die letzte an die Datenbank verplante Transaktion gespeichert wird.

  Der Zeitpunkt kann eine Oracle System Change Number (SCN) oder ein Datum und eine Uhrzeit (yyyy-mm-dd:hh:mm:ss) sein. Bei SnapManager wird die 24-Stunden-Zeit verwendet.

- Restore aus Backups im Primärspeicher (lokale Backups).
- Stellen Sie das Backup mit SnapManager wieder her, oder verwenden Sie SnapManager für die Wiederherstellung des Backups und verwenden Sie ein anderes Tool wie Recovery Manager (RMAN) zur Wiederherstellung der Daten.
- Wiederherstellung von Backups von alternativen Orten aus
- Stellen Sie geschützte Backups aus dem sekundären Storage (Remote Backups) und von einem alternativen Speicherort mithilfe der Spezifikationsdatei für die Wiederherstellung wieder her.

Sie können ein Backup, das von einer früheren Version von SnapManager erstellt wurde, mit SnapManager 3.0 und höher wiederherstellen.

SnapManager bietet außerdem die Möglichkeit, ASM-Datenbanken (Automatic Storage Management) wiederherzustellen. Eine ASM-Laufwerksgruppe kann von mehreren Datenbanken gemeinsam genutzt werden. Daher können Sie nicht auf eine ältere Snapshot Kopie der Festplattengruppe zurücksetzen, da sie alle Datenbanken zurücksetzen würde. Bei herkömmlichen Lösungen für Restores kommt es auf den Host zu allen Blöcken, die die Datenbank bilden, die vom Storage-System zum Host verschoben werden und anschließend zurück zum Storage-System. SnapManager entlastet diesen Overhead, da es die Möglichkeit gibt, nur die erforderlichen Daten innerhalb der ASM-Festplattengruppe wiederherzustellen, ohne über den Host zu gehen.

Administratoren können Restore- oder Recovery-Vorgänge über die grafische Benutzeroberfläche von SnapManager oder über die Befehlszeilenschnittstelle (CLI) durchführen.

Verwandte Informationen

Backup von Datenbanken

Der Smo Backup Restore Befehl

Was ist Datenbank-Restore

SnapManager ermöglicht die Durchführung von Volume- oder dateibasierten Backup- und Restore-Vorgängen.

In der folgenden Tabelle werden die Wiederherstellungsmethoden beschrieben:

Wiederherstellungsprozess	Details
Schnelle, Volume-basierte Restores (vom Primärspeicher)	SnapManager stellt durch die Wiederherstellung eines vollständigen Volumes die Datendateien einer Datenbank wieder her. Dieser Standardprozess ist die schnellste Methode zum Wiederherstellen Ihrer Datenbank.
Dateibasierte Restores	Storage-seitige Wiederherstellung eines vollständigen File-Systems (von primärem oder sekundärem): SnapManager führt eine vollständige Wiederherstellung der Logical Unit Number (LUN) durch.
Storage-seitige Dateiwiederherstellung: SnapManager führt eine einzelne File Snap Restore (SFSR) in einer NAS-Umgebung oder eine Teildateiwiederherstellung (PFSR) in einer ASM-Umgebung (Automatic Storage Management) durch. In einem SFSR werden die Dateien oder LUNs, die die geschützten Objekte darstellen, wiederhergestellt. Ein PFSR wird aus dem lokalen Backup ausgeführt, wenn sich das Dateisystem und das Layout des Dateisystems seit dem letzten Backup nicht geändert haben.	Wiederherstellung von Host-seitigen Dateikopien (von primärem oder sekundärem): SnapManager klont den lokalen Backup mit entweder einer LUN oder einem FlexClone. Der Klon ist gemountet und dann kopiert SnapManager die Host-Dateien aus dem Klon in das aktive Dateisystem.

Die Standardeinstellung ist der schnelle Wiederherstellungsprozess, Administratoren können jedoch einen beliebigen Typ auswählen. Während des schnellen Wiederherstellungsprozesses stellt SnapManager Informationen zu Bedingungen zur Verfügung, die das Abschließen des schnellen Wiederherstellungsprozesses sowie zu Bedingungen, die sich auf die schnelle Wiederherstellung auswirken können, die jedoch von Administratoren ignoriert werden können, wenn sie den Prozess fortsetzen möchten.

Sie können ein Backup nicht aus dem sekundären Speicher wiederherstellen, wenn auch das Backup auf dem primären Speicher vorhanden ist.

Wenn der schnelle Restore-Vorgang abgeschlossen ist, führt SnapManager die folgenden Aufgaben aus:

- Gibt aktuellere Backups (nach Wiederherstellung des Backups erstellt) in demselben Profil frei, da die Snapshot Kopien nicht mehr im Primär-Storage vorhanden sind.
- Löscht alle Snapshot-Kopien für Backups im selben Profil, in dem alle Snapshot-Kopien automatisch durch den schnellen Wiederherstellungsprozess gelöscht wurden.

  Dadurch wird verhindert, dass Backups teilweise freigegeben werden. Beispiel: Backup_A wurde zuerst erstellt und dann Backup_B erstellt. Jeder verfügt über eine Snapshot Kopie für die Datendateien und eine für die Archivprotokolle. Nachdem SnapManager Backup_A mithilfe des schnellen Wiederherstellungsprozesses wiederhergestellt hat, löscht SnapManager automatisch die Snapshot Kopie der Datendatei aus Backup_B. Da das Archivprotokoll im schnellen Restore nicht wiederhergestellt wird, muss SnapManager nach Abschluss des schnellen Restore-Prozesses die Snapshot-Kopie von Backup_B der Archivprotokolle löschen.

Schnelle Wiederherstellung

Der Name der schnellen Wiederherstellung oder Volume-basierten Wiederherstellung ist so hoch, da es sich um die schnellstmögliche Wiederherstellungsmethode handelt. Das gesamte Storage-System-Volume wird auf eine Snapshot Kopie zurückgesetzt. Auf Storage-Ebene erfolgt diese Wiederherstellung nahezu verzögerungsfrei. Eine Wiederherstellung eines Volumes kann jedoch die folgenden negativen Folgen haben und muss daher mit Vorsicht verwendet werden:

- Das gesamte Storage-seitige Volume wird zurückgesetzt, einschließlich:
  - Dateien, die nicht als Teil des Backups betrachtet wurden
  - Andere Dateien, Filesysteme oder LUNs auf dem Volume
- Alle Snapshot Kopien, die nach der Snapshot Kopie erstellt wurden, auf die das Volume zurückgesetzt wird, werden gelöscht.

  Sie können zum Beispiel das Backup am Dienstag nicht mehr wiederherstellen, wenn Sie das Volume am Montag wiederhergestellt haben.

- Beziehungen zu sekundären Storage-Systemen werden beschädigt, wenn die wiederhergestellte Snapshot Kopie älter als die zugrunde liegende Snapshot Kopie in der Beziehung ist.

Storage-seitig komplette Wiederherstellung des Dateisystems

Wenn keine Volume-Wiederherstellung möglich ist, wird ein Storage-seitiges File-System wiederhergestellt, das gesamte File-System kann jedoch auf dem Storage-System wiederhergestellt werden.

Wenn eine Storage-seitige Wiederherstellung eines Dateisystems durchgeführt wird, geschieht Folgendes:

- In einer SAN-Umgebung sind alle vom Filesystem verwendeten LUNs (und ggf. die zugrunde liegende Volume-Gruppe) auf dem Storage-System wiederhergestellt.
- In einer NAS-Umgebung wird jede Datei im Filesystem auf dem Storage-System wiederhergestellt.

  In NAS-Umgebungen bietet dieser Wiederherstellungsmechanismus keine zusätzlichen Vorteile bei der Wiederherstellung von Dateien auf Storage-Seite.

Wenn eine Storage-seitige Wiederherstellung des Filesystems erfolgt, hängt vom Speicherort ab:

- Bei SnapManager-Restores von primären Storage-Systemen werden die LUNs (SAN) oder Dateien (NAS) an Ort und Stelle über SFSR wiederhergestellt.
- Wenn SnapManager aus sekundären Storage-Systemen wiederhergestellt wird, werden LUNs (SAN) oder Dateien (NAS) von sekundären Storage-Systemen über das Netzwerk zurück in das primäre Storage-System kopiert.

Da das Filesystem vollständig wiederhergestellt ist, werden auch Dateien, die nicht zum Backup gehören, zurückgesetzt. Eine Überschreibung ist erforderlich, wenn Dateien, die nicht Teil der Wiederherstellung sind, im Dateisystem vorhanden sind, das wiederhergestellt wird.

Datei-Restore auf Storage-Seite

Eine Speicherseitige Dateiwiederherstellung wird manchmal durchgeführt, wenn eine speicherseitige Dateisystemwiederherstellung nicht möglich ist. Bei einer File-Wiederherstellung ohne Storage-Systeme werden einzelne Dateien innerhalb eines Filesystems direkt in den Storage-Systemen wiederhergestellt.

Diese Art von Wiederherstellung kann nur in NFS Umgebungen durchgeführt werden.

In ASM-Umgebungen kann die Wiederherstellung von Dateien auf Speicherseite nur durchgeführt werden, wenn die folgenden Bedingungen gelten:

- Erweiterungen der zugrunde liegenden Datei haben sich seit der Sicherung nicht geändert (beispielsweise wurde die Datei nicht geändert und die Ausbalancierung der Festplatte wurde nicht vorgenommen).
- Sie führen ein Restore von einem primären Storage-System aus. (Diese wird nicht unterstützt, wenn die Wiederherstellung von sekundären Speichersystemen aus erfolgt.)

Wenn eine Wiederherstellung von Dateien auf Storage-Seite durchgeführt wird, geschieht Folgendes:

- Wenn SnapManager NFS-Dateien aus den primären Storage-Systemen wiederherstellt, werden die einzelnen Dateien mittels SFSR wiederhergestellt.
- Wenn SnapManager NFS-Dateien aus sekundären Storage-Systemen wiederherstellt, werden die einzelnen Dateien über das Storage-Netzwerk zurück in das primäre Storage-System kopiert.
- Beim Wiederherstellen von ASM-Dateien aus den primären Storage-Systemen werden die einzelnen Dateien an Ort und Stelle wiederhergestellt, indem nur die Bytes in den zugrunde liegenden LUNs wiederhergestellt werden, die zur Wiederherstellung der Dateien erforderlich sind (der Rest der Bytes in den LUNs bleibt erhalten). Die Speichersystemtechnologie, die zum Wiederherstellen von LUNs verwendet wird, wird teilweise PFSR genannt.

Host-seitiges Datei-Restore

Eine Wiederherstellung von Host-seitigen Dateikopien dient als letztes Mittel in SAN-Umgebungen, wenn keine schnelle Wiederherstellung, eine rasche Wiederherstellung auf Storage-Seite eines Filesystems und die Wiederherstellung von Dateien auf Storage-Seite durchgeführt werden kann.

Zur Wiederherstellung einer Host-seitigen Dateikopie gehören die folgenden Aufgaben:

- Klonen des Speichers
- Verbinden des geklonten Speichers mit dem Host
- Kopieren von Dateien aus den Klon-Dateisystemen zurück in die aktiven Dateisysteme
- Trennen des Klonspeichers vom Host
- Löschen des Klonspeichers

Beim Restore aus dem sekundären Storage versucht SnapManager zunächst, Daten direkt aus dem sekundären Storage-System in das primäre Storage-System (ohne Beteiligung des Hosts) wiederherzustellen. Wenn SnapManager diese Art der Wiederherstellung nicht ausführen kann (z. B. wenn Dateien nicht Teil der Wiederherstellung in einem Dateisystem vorhanden sind), führt SnapManager die Wiederherstellung der Host-seitigen Dateikopie durch. SnapManager verfügt über zwei Methoden zur Wiederherstellung einer Host-seitigen Dateikopie aus dem sekundären Storage. Die Methode SnapManager auswählt ist in der Datei smo.config konfiguriert.

- Direkt: SnapManager klont die Daten auf dem sekundären Storage, bindet die geklonten Daten vom sekundären Storage-System an den Host und kopiert dann Daten aus dem Klon in die aktive Umgebung. Dies ist die standardmäßige sekundäre Zugriffsrichtlinie.
- Indirekt: SnapManager kopiert die Daten zunächst auf ein temporäres Volume im Primärspeicher, bindet die Daten dann vom temporären Volume an den Host und kopiert dann Daten aus dem temporären Volume in die aktive Umgebung. Diese sekundäre Zugriffsrichtlinie sollte nur verwendet werden, wenn der Host keinen direkten Zugriff auf das sekundäre Speichersystem hat. Bei Wiederherstellungen mit dieser Methode dauert die Methode doppelt so lange wie die Richtlinie für den direkten sekundären Zugriff, da zwei Kopien der Daten erstellt werden.

Die Entscheidung, ob die direkte oder indirekte Methode verwendet werden soll, wird durch den Wert des Parameters restore.secondaryAccessPolicy in der Konfigurationsdatei smo.config gesteuert. Die Standardeinstellung lautet „direkt“.

Richtlinien für den Zeitpunkt, zu dem Sie schnelle Wiederherstellungen verwenden können

Spezifische Regeln gelten für den Einsatz von schneller Wiederherstellung, um eine optimale Wiederherstellungsleistung zu erreichen. In manchen Fällen können Sie kein schnelles Restore verwenden.

Zur Erzielung einer optimalen Restore-Performance (Volume-Wiederherstellung oder vollständige Festplattengruppenwiederherstellung) müssen folgende Regeln eingehalten werden:

- Nur vollständige Restores von vollständigen Backups können schnell wiederhergestellt werden.
- Nur Datendateien können schnell wiederhergestellt werden.
- Datendateien müssen die einzigen Dateien eines Volumes sein, um schnell wiederhergestellt werden zu können.

  Auch wenn temporäre Datendateien auf dem Volume liegen können, müssen Steuerdateien, Protokolle, pfiles oder andere Dateien auf einem separaten Volume von den Datendateien gespeichert werden. Sie müssen eine Oracle-Datenbank mit Datendateien auf einem separaten Volume von Kontrolldateien, archivierten Protokollen und Online-Protokolldateien einrichten.

- Das Volume muss Datendateien für nur eine Datenbank enthalten.
- Es können mehrere Dateisysteme verwendet werden, aber die Dateien in diesen Dateisystemen müssen Datendateien für nur eine Datenbank sein.
- Für ASM-Datenbanken muss jede Datenbank eine eigene ASM-Laufwerksgruppe verwenden, und die ASM-Datenbank kann keinen Speicher mit einer anderen ASM-Datenbank teilen.

> Um zu prüfen, ob ein zuvor erstelltes Backup mithilfe der schnellen Wiederherstellung wiederhergestellt werden kann, kann die Option -Preview des Befehls smo Backup Restore verwendet werden.

Die schnelle Wiederherstellung kann in den folgenden Fällen nicht verwendet werden:

- Bei teilweise Backups
- Auf Backups aus dem sekundären Storage, wenn das Backup auch auf dem primären Speicher vorhanden ist

  Diese können nicht mithilfe der Datei- oder Volume-basierten Wiederherstellung wiederhergestellt werden.

- Auf Backups, die mit SnapVault gesichert sind

  Der schnelle Wiederherstellungsprozess kann nicht für Backups verwendet werden, die vor dem letzten geschützten Backup erstellt wurden. Sie können jedoch den schnellen Wiederherstellungsprozess für Backups verwenden, die nach dem letzten geschützten Backup erstellt wurden. Denken Sie beispielsweise an Backups A, B und C. B ist das letzte Backup, das mit SnapVault auf den sekundären Storage übertragen wird. Sie können B und C schnell wiederherstellen, aber Sie können A nicht schnell wiederherstellen, da sie vor dem letzten geschützten Backup erstellt wurde. SnapVault benötigt eine Basis-SnapVault, um den Zeitunterschied zu berechnen und zum sekundären Storage zu senden, wenn das nächste Backup in den sekundären Storage übertragen wird. Das letzte geschützte Backup fungiert als

Basis-Snapshot Kopie. Daher verhindert ein schneller Wiederherstellungsprozess, dass SnapVault die Baseline erkennen kann.

- FlexClones oder LUN-Klone, die Snapshot Kopien verwenden, die nach der Snapshot Kopie, auf die das Volume zurückgesetzt wird, erstellt wurden

  Beispielsweise können die Klone auf ein späteres Backup zurückzuführen sein, das durch SnapManager gemountet oder geklont wird.

- LUNs, die nicht Teil der aktiven SnapDrive Snapshot Kopie sind

Sie können keine schnelle Wiederherstellung zusammen mit anderen Arten von Wiederherstellungen für dasselbe Backup durchführen. Wenn beispielsweise ein Datenvolumen mit dem schnellen Restore-Prozess wiederhergestellt werden kann, aber ein anderes Daten-Volume kann nicht, so wird es mit dem schnellen Restore-Prozess auch nicht wiederhergestellt. In diesem Fall können Sie eine dateibasierte Wiederherstellung auswählen.

Darüber hinaus sollten Sie die folgenden Punkte zu Datenbank-Wiederherstellungen in Betracht ziehen:

- SnapManager stellt niemals Archivprotokolle oder Wiederherstellungsprotokolle wieder her, bindet aber das Backup von Archivprotokolldateien und verwendet sie für die Wiederherstellung.
- SnapManager stellt niemals Dateien durch Volume Restore unter Kontrolle.
- Wenn Sie Steuerdateien und Datendateien wiederherstellen möchten, führt SnapManager die Wiederherstellung in zwei Schritten durch.

  SnapManager stellt zuerst die Kontrolldateien und dann die Datendateien wieder her.

- Wenn SnapManager temporäre Dateien in demselben Volume wie die standardmäßigen Tablespaces findet, müssen Sie zur Wiederherstellung auf Volume-Ebene keine Überschreibung erstellen.

  Nach einer Volume-Wiederherstellung wird der TEMP Tablespace wieder online gestellt.

Verwandte Informationen

Empfohlene allgemeine Datenbanklayouts und Speicherkonfigurationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Vor- und Nachteile bei schneller Wiederherstellung

DBAs sollten sich der vor- und Nachteile der Verwendung von Volume-basierten schnellen Restores bewusst sein.

Das Wiederherstellen von Datenbank-Backups mithilfe von schnellen Wiederherstellungen bietet die folgenden Vorteile:

- Volume-basierte Restores reduzieren den Zeitaufwand für die Wiederherstellung von Backups.
- SnapManager bietet schnelle Überprüfung der Teilnahmevoraussetzungen für eine Wiederherstellung. SnapManager analysiert das Datenbank-Backup und zeigt Informationen darüber an, ob es das Volume-basierte Restore durchführen kann.
- Sie können eine Vorschau des Wiederherstellungsvorgangs anzeigen und entscheiden, ob Sie den empfohlenen Pfad verwenden oder die Empfehlung mit Ihrem ausgewählten Prozess überschreiben möchten.

Die Wiederherstellung von Datenbank-Backups mit schnellen Restores hat die folgenden Nachteile:

- Das gesamte Filesystem wurde zurückgesetzt, auch Dateien, die nicht als Teil des Backups betrachtet wurden. Andere Dateien, Filesysteme oder LUNs auf dem Volume werden ebenfalls zurückgesetzt.
- SnapManager entfernt alle Snapshot Kopien, die nach dem Zurücksetzen des Snapshots erstellt wurden. In Tat verlieren Sie den Verlauf nach dem Datum der Snapshot Kopie. Beispielsweise können Sie das Backup am Dienstag nicht wiederherstellen, wenn Sie bereits das Backup am Montag wiederhergestellt haben.

Sie können die Nachteile vermeiden, indem Sie folgende Empfehlungen befolgen:

- Optimieren Sie das Datenbank-Layout anhand der Best Practices.
- Sicherung von Backups auf Sekundärspeicher Wenn Sie jedoch Snapshot-Kopien aus dem Primärspeicher löschen, können Sie keine schnellen Wiederherstellungen verwenden, um sie aus dem Sekundärspeicher wiederherzustellen.

Überprüfung der Teilnahmevoraussetzungen für eine schnelle Wiederherstellung

Wenn Sie eine schnelle Wiederherstellung eines Backups durchführen möchten, führt SnapManager zunächst eine Eignungsüberprüfung durch, um festzustellen, ob der schnelle Restore-Prozess verwendet werden kann.

SnapManager bietet folgende Arten von Prüfungen:

- Obligatorische Prüfungen: SnapManager kann den Schnellwiederherstellungsprozess nur dann durchführen, wenn alle Bedingungen unter diesem Prüfvorgang erfüllt sind.
- Übersteuerbare Prüfungen: Wenn die Bedingungen unter dieser Prüfung fehlschlagen, können Administratoren die Prüfung überschreiben, um einen schnellen Wiederherstellungsprozess zu erzwingen. Sie müssen diese Prüfungen jedoch mit Vorsicht überschreiben.

In der folgenden Tabelle sind die Probleme aufgeführt, die möglicherweise auftreten können, und es wird angegeben, ob die Überprüfung der Berechtigung zur schnellen Wiederherstellung überschrieben werden kann:

Problem	Pass erforderlich	Details
ACFS, Voting Disk oder OCR ist in der ASM-Laufwerksgruppe in 11gR2 vorhanden	Ja.	Eine schnelle Wiederherstellung ist nicht möglich. Auflösung: Keine Kann nicht überschrieben werden.
Nur mit SnapManager 3.0 oder neuer erstellte Backups können schnell wiederhergestellt werden	Ja.	Kann nicht überschrieben werden.
Nur mit SnapDrive für UNIX 4.0 oder höher erstellte Snapshot Kopien können schnell wiederhergestellt werden	Ja.	Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Volumen ist ein Wurzelvolumen	Ja.	Das wiederherzustellende Volume ist ein Root-Volume im Storage-System. Lösung: Verwenden Sie das Root-Volume nicht auf dem Speichersystem. Kann nicht überschrieben werden.
Die Volume-Wiederherstellung ist unter Windows nicht verfügbar	Ja.	Das wiederherzustellende Volume ist ein Root-Volume im Storage-System. Auflösung: Keine Kann nicht überschrieben werden.
Die Volume-Wiederherstellung ist deaktiviert	Ja.	Die Volume-Wiederherstellung wurde deaktiviert. Auflösung: Aktivieren Sie die Volume-Wiederherstellung durch Auswahl verschiedener Optionen beim Starten der Wiederherstellung. Verwenden Sie nicht -fast -off auf der Befehlszeilenschnittstelle. Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Kontrollieren Sie Dateien und Datendateien auf demselben Volume	Ja.	Bei Online-Backups können Kontrolldateien und Datendateien nicht auf demselben Volume liegen, da SnapManager zwei Snapshot Kopien des Volumes erstellt (eine davon, bei denen die Datendateien im Hot-Backup-Modus konsistent sind). Und einer, bei dem die Backup-Kontrolldateien nach Abschluss des Hot-Backup-Modus konsistent sind). Die Wiederherstellung des Volume wird auf die erste Snapshot Kopie zurückgesetzt, die die zweite Snapshot Kopie mit den Backup-Kontrolldateien löscht. Wenn eine Daten-File-only Wiederherstellung stattfindet, werden die Kontrolldateien in einen inkonsistenten Zustand zurückgesetzt und SnapManager stellt die Backup-Kontrolldatei wieder her und öffnet dann die Datenbank mit der Option Resetlogs, was nicht das gewünschte Verhalten ist. Lösung: Migrieren von Kontrolldateien und Datendateien auf separate Dateisysteme, die nicht dasselbe zugrunde liegende Volume nutzen. Dies hilft nicht bei der Wiederherstellung, bei der die Prüfung fehlgeschlagen ist, sondern wird zukünftigen Backup-Wiederherstellungsvorgängen helfen. Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Archivprotokolle und Datendateien dürfen nicht auf demselben Volume vorhanden sein	Ja.	Datenbank-Archivprotokolle und Datendateien befinden sich in Filesystemen, die von demselben Storage-System-Volume gesichert sind. Falls eine Wiederherstellung eines Volumes durchgeführt wurde, kann SnapManager die Datenbank nach der Wiederherstellung eines Online-Backups nicht öffnen, weil die archivierte Protokolldatei, die geschrieben wird, nachdem die Datenbank aus dem Hot-Backup-Modus entfernt wurde, nicht verfügbar ist. Darüber hinaus wären Sie nicht in der Lage, spätere Transaktionen durchzuführen, die möglicherweise in den Archiv-Log-Dateien waren. Lösung: Migration von Archivprotokollen und Datendateien auf separate Filesysteme, die nicht dasselbe zugrunde liegende Storage-System-Volume nutzen Dies hilft nicht bei der Wiederherstellung, bei der die Prüfung fehlgeschlagen ist, sondern wird zukünftigen Backup-Wiederherstellungsvorgängen helfen. Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Online-Protokolle und Datendateien dürfen nicht auf demselben Volume vorhanden sein	Ja.	Datenbank Online-Wiederherstellungsprotokolle und Datendateien befinden sich in Filesystemen, die von demselben Storage-System-Volume gesichert sind. Wenn ein Volume wiederhergestellt wurde, kann die Recovery die Online-Wiederherstellungsprotokolle nicht verwenden, weil sie zurückgesetzt wurden. Lösung: Migrieren Sie Online-Redo-Protokolle und -Datendateien auf separate Filesysteme, die nicht dasselbe zugrunde liegende Storage-System-Volume nutzen. Dies hilft nicht bei der Wiederherstellung, bei der die Prüfung fehlgeschlagen ist, sondern wird zukünftigen Backup-Wiederherstellungsvorgängen helfen. Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Dateien im Filesystem, nicht Teil des Wiederherstellungsumfangs werden zurückgesetzt	Ja.	Dateien, die auf dem Host sichtbar sind, außer den wiederherzustellenden Dateien, sind in einem Dateisystem auf dem Volume vorhanden. Wenn eine schnelle Wiederherstellung eines Filesystems oder eine Wiederherstellung eines Storage-Systems durchgeführt wurde, würden die auf dem Host sichtbaren Dateien beim Erstellen der Snapshot Kopie auf den ursprünglichen Inhalt zurückgesetzt. Wenn SnapManager 20 oder weniger Dateien erkennt, werden sie in der Eignungsüberprüfung aufgeführt. Andernfalls zeigt SnapManager eine Meldung an, dass Sie das Dateisystem untersuchen sollten. Auflösung: Migrieren Sie die Dateien, die nicht von der Datenbank verwendet werden, auf ein anderes Dateisystem, das ein anderes Volume verwendet. Alternativ können Sie die Dateien löschen. Wenn SnapManager den Dateizweck nicht bestimmen kann, können Sie den Prüffehler überschreiben. Wenn Sie die Prüfung überschreiben, werden die Dateien, die sich nicht im Wiederherstellungsbereich befinden, zurückgesetzt. Setzen Sie diese Prüfung nur außer Kraft, wenn Sie sicher sind, dass das Zurücksetzen der Dateien nichts beeinträchtigt.

Problem	Pass erforderlich	Details
Dateisysteme in der angegebenen Volume-Gruppe sind nicht Teil des Wiederherstellungsumfangs	Nein	Mehrere Dateisysteme befinden sich in derselben Volume-Gruppe, aber nicht alle Dateisysteme müssen wiederhergestellt werden. Mit Storage-seitigem Filesystem Restore und schnellem Restore können keine einzelnen Dateisysteme innerhalb einer Volume-Gruppe wiederhergestellt werden, da die von der Volume-Gruppe verwendeten LUNs Daten aus allen Dateisystemen enthalten. Alle Dateisysteme innerhalb einer Volume-Gruppe müssen gleichzeitig wiederhergestellt werden, um eine schnelle Wiederherstellung oder eine speicherseitige Filesystem-Wiederherstellung zu verwenden. Wenn SnapManager 20 oder weniger Dateien erkennt, listet SnapManager diese in der Eignungsprüfung auf. Andernfalls bietet SnapManager eine Meldung, die Sie untersuchen sollten das Dateisystem. Auflösung: Migrieren Sie die Dateien, die nicht von der Datenbank verwendet werden, auf eine andere Volume-Gruppe. Alternativ können Sie die Dateisysteme in der Volume-Gruppe löschen. Kann überschrieben werden.

Problem	Pass erforderlich	Details
Host-Volumes in einer bestimmten Volume-Gruppe werden nicht Teil des Wiederherstellungsumfangs zurückgesetzt	Nein	Mehrere Host Volumes (logische Volumes) befinden sich in derselben Volume-Gruppe, jedoch werden nicht alle Host Volumes benötigt, um wiederhergestellt zu werden. Diese Prüfung ähnelt den Dateisystemen in der Volume-Gruppe, die nicht Teil des Wiederherstellungsumfangs sind, kann zurückgesetzt werden, außer dass die anderen Host-Volumes in der Volume-Gruppe nicht als Dateisysteme auf dem Host gemountet werden. Lösung: Migrieren Sie Host-Volumes, die von der Datenbank verwendet werden, auf eine andere Volume-Gruppe. Oder löschen Sie die anderen Host Volumes in der Volume-Gruppe. Wenn Sie die Prüfung außer Kraft setzen, werden alle Host-Volumes in der Volume-Gruppe wiederhergestellt. Setzen Sie diese Prüfung nur außer Kraft, wenn Sie sicher sind, dass sich die Zurücksetzung der anderen Host-Volumes nachteilig auf nichts auswirkt.
Die DateiExtents haben sich seit dem letzten Backup geändert	Ja.	Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Zugeordnete LUNs in Volume sind nicht im Rahmen der Wiederherstellung zurückgesetzt	Ja.	LUNs, die nicht über die im Volume wiederherzustellenden LUNs liegen, sind derzeit einem Host zugeordnet. Eine Volume-Wiederherstellung kann nicht durchgeführt werden, da andere Hosts oder Applikationen, die diese LUNs verwenden, instabil werden. Wenn die LUN-Namen mit einem Unterstrich und einem Integer-Index enden (z. B. _0 oder _1), sind diese LUNs normalerweise Klone anderer LUNs innerhalb desselben Volumes. Es ist möglich, dass ein weiteres Backup der Datenbank angehängt ist oder ein Klon eines anderen Backups existiert. Lösung: Migrieren von LUNs, die nicht von der Datenbank auf ein anderes Volume verwendet werden. Wenn es sich bei den zugeordneten LUNs um Klone handelt, suchen Sie nach gemounteten Backups derselben Datenbank oder Klone der Datenbank, und mounten Sie den Backup oder entfernen Sie den Klon. Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Nicht zugeordnete LUNS im Volume sind nicht Teil des Wiederherstellungsumfangs	Nein	Andere LUNs als die LUNs, die im Volume wiederhergestellt werden sollen, sind vorhanden. Diese LUNs sind derzeit keinem Host zugeordnet, daher werden durch die Wiederherstellung der LUNs keine aktiven Prozesse unterbrochen. Die Zuordnung der LUNs kann jedoch vorübergehend aufgehoben werden. Lösung: Migrieren von LUNs, die nicht von der Datenbank genutzt werden, auf ein anderes Volume oder Löschen der LUNs Wenn Sie diese Prüfung überschreiben, setzt die Volume-Wiederherstellung diese LUNs in den Status zurück, ab dem die Snapshot Kopie erstellt wurde. Wenn die LUN beim Erstellen der Snapshot Kopie nicht vorhanden war, ist die LUN nach der Wiederherstellung des Volume nicht vorhanden. Setzen Sie diese Prüfung nur außer Kraft, wenn Sie sicher sind, dass die Zurücksetzung der LUNs nichts beeinträchtigt.

Problem	Pass erforderlich	Details
LUNs, die in der Snapshot Kopie des Volume vorhanden sind, sind möglicherweise nicht konsistent, wenn zurückgesetzt wird	Nein	Während der Erstellung von Snapshot Kopien existierten andere LUNs als die, für die die Snapshot Kopie angefordert wurde, im Volume. Diese anderen LUNs haben möglicherweise keinen konsistenten Status. Lösung: Migrieren von LUNs, die nicht von der Datenbank genutzt werden, auf ein anderes Volume oder Löschen der LUNs Dies hilft nicht beim Wiederherstellungsvorgang, bei dem die Prüfung fehlgeschlagen ist, aber Wiederherstellungen zukünftiger Backups, die nach dem Verschieben oder Löschen der LUNs erstellt wurden, helfen können. Wenn Sie diese Prüfung außer Kraft setzen, werden die LUNs in den inkonsistenten Status zurückgesetzt, mit dem die Snapshot Kopie erstellt wurde. Setzen Sie diese Prüfung nur außer Kraft, wenn Sie sicher sind, dass die Zurücksetzung der LUNs nichts beeinträchtigt.
Neue Snapshot Kopien enthalten Volume-Klon	Ja.	Klone wurden von Snapshot Kopien erstellt, die nach der Wiederherstellung der Snapshot Kopie erstellt wurden. Da zu einem Zeitpunkt eine Wiederherstellung eines Volume spätere Snapshot Kopien gelöscht wird und eine Snapshot Kopie nicht gelöscht werden kann, wenn er über einen Klon verfügt, kann eine Wiederherstellung des Volumes nicht durchgeführt werden. Auflösung: Klone späterer Snapshot Kopien löschen Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Neuere Backups werden angehängt	Ja.	Backups, die nach der Wiederherstellung des Backups erstellt wurden, werden gemountet. Da bei einer Volume-Wiederherstellung spätere Snapshot Kopien gelöscht werden, kann eine Snapshot Kopie nicht gelöscht werden, wenn dieser über einen Klon verfügt, bei einem Backup-Mount-Vorgang wird geklonter Storage erstellt und eine Volume-Wiederherstellung nicht möglich ist. Lösung: Heben Sie die Bereitstellung des späteren Backups auf, oder stellen Sie die Wiederherstellung aus einem Backup nach dem gemounteten Backup wieder her. Kann nicht überschrieben werden.
Klone neuerer Backups sind vorhanden	Ja.	Backups, die nach der Wiederherstellung des Backups erstellt wurden, wurden geklont. Da später Snapshot Kopien durch eine Volume-Wiederherstellung gelöscht werden und eine Snapshot Kopie nicht gelöscht werden kann, wenn er über einen Klon verfügt, kann keine Wiederherstellung des Volumes durchgeführt werden. Lösung: Löschen Sie den Klon des neueren Backups oder führen Sie Restores aus einem Backup durch, das nach den Klonen bei den Backups erstellt wurde. Kann nicht überschrieben werden.

Problem	Pass erforderlich	Details
Neue Snapshot Kopien des Volume gingen verloren	Nein	Durch die Wiederherstellung eines Volumes werden alle Snapshot Kopien gelöscht, die nach der Snapshot Kopie, die das Volume wiederhergestellt wird, erstellt wurden. Wenn SnapManager eine spätere Snapshot Kopie im selben Profil einem SnapManager Backup zuordnen kann, wird die Meldung „neuere Backups werden freigegeben oder gelöscht“ angezeigt. Wenn SnapManager eine spätere Snapshot Kopie nicht im selben Profil einem SnapManager Backup zuordnen kann, wird diese Meldung nicht angezeigt. Lösung: Wiederherstellung aus einem späteren Backup oder Löschen der späteren Snapshot Kopien Kann überschrieben werden.

Problem	Pass erforderlich	Details
Neuere Backups werden freigegeben oder gelöscht	Nein	Durch die Wiederherstellung eines Volumes werden alle Snapshot Kopien gelöscht, die nach der Snapshot Kopie, auf die das Volume wiederhergestellt wird, erstellt wurden. Daher werden alle Backups, die nach dem wiederhergestellten Backup erstellt wurden, entweder gelöscht oder freigegeben. Spätere Backups werden in folgenden Szenarien gelöscht: • Der Sicherungsstatus ist nicht GESCHÜTZT • Exsave.alwayFreeExpiredBackups sind in smo.config falsch Backups werden später in folgenden Szenarien freigegeben: • Der Backup-Status IST GESCHÜTZT • Consave.alwayFreeExpiredBackups sind in smo.config richtig Lösung: Wiederherstellung aus einem späteren Backup oder kostenlose oder löschen Sie später Backups. Wenn Sie diese Prüfung außer Kraft setzen, werden Backups, die nach dem wiederherzustellenden Backup erstellt wurden, gelöscht oder freigegeben.

Problem	Pass erforderlich	Details
SnapMirror Beziehung für Volume wurde verloren	Ja (wenn RBAC deaktiviert ist oder Sie keine RBAC-Rechte haben)	Durch das Wiederherstellen eines Volume auf eine Snapshot Kopie vor der Basis-Snapshot Kopie in einer SnapMirror Beziehung wird die Beziehung zerstört. Lösung: Wiederherstellung aus einem Backup, das nach der Basis-Snapshot Kopie der Beziehung erstellt wurde Alternativ können Sie die Storage-Beziehung manuell unterbrechen (und dann die Beziehung nach Abschluss der Wiederherstellung erneut erstellen und neu erstellen). Kann überschrieben werden, wenn RBAC aktiviert ist und Sie über RBAC verfügen.
Die SnapVault-Beziehung für das Volume geht verloren, wenn der schnelle Wiederherstellungsprozess eingetreten ist	Ja (wenn RBAC deaktiviert ist oder Sie keine RBAC-Rechte haben)	Durch das Wiederherstellen eines Volumes auf eine Snapshot Kopie vor der Basis-Snapshot Kopie in einer SnapVault Beziehung wird die Beziehung zerstört. Lösung: Wiederherstellung aus einem Backup, das nach der Basis-Snapshot Kopie der Beziehung erstellt wurde Alternativ können Sie die Storage-Beziehung manuell unterbrechen (und dann die Beziehung nach Abschluss der Wiederherstellung erneut erstellen und neu erstellen). Kann nicht überschrieben werden. Wenn RBAC aktiviert ist und Sie über die Berechtigung zur rollenbasierten Zugriffssteuerung verfügen.

Problem	Pass erforderlich	Details
NFS-Dateien in Volume werden nicht Teil des Wiederherstellungsumfangs zurückgesetzt	Nein	Dateien, die im Storage-System-Volume vorhanden sind und auf dem Host nicht sichtbar sind, werden bei der Wiederherstellung eines Volumes zurückgesetzt. Auflösung: Migrieren Sie Dateien, die nicht von der Datenbank verwendet werden, auf ein anderes Volume oder löschen Sie die Dateien. Kann überschrieben werden. Wenn Sie diese Prüfung nicht überschreiben, werden die LUNs gelöscht.
CIFS-Freigaben für Volume sind vorhanden	Nein	Das wiederherzustellende Volume verfügt über CIFS-Freigaben. Während der Volume-Wiederherstellung greifen andere Hosts möglicherweise auf Dateien auf dem Volume zu. Lösung: Entfernen Sie nicht benötigte CIFS Shares. Kann überschrieben werden.
Wiederherstellung von einem alternativen Speicherort	Ja.	Für den Wiederherstellungsvorgang wurde eine Wiederherstellungsspezifikation bereitgestellt, die angibt, dass die Dateien von einem anderen Speicherort wiederhergestellt werden. Nur Werkzeuge für die Erstellung von Kopien auf Host-Seite können verwendet werden, um sie von einem alternativen Speicherort wiederherzustellen. Auflösung: Keine. Kann nicht überschrieben werden.
Die Wiederherstellung eines speicherseitigen Filesystems wird in einer RAC ASM-Datenbank nicht unterstützt	Ja.	Kann nicht überschrieben werden.

Backup Recovery

In SnapManager müssen gleichzeitig die Wiederherstellungs- und Recovery-Vorgänge ausgeführt werden. Sie können keinen Wiederherstellungsvorgang ausführen und anschließend einen SnapManager-Wiederherstellungsvorgang später durchführen.

In SnapManager 3.2 oder einer älteren Version können Sie entweder mit SnapManager das Backup wiederherstellen und wiederherstellen, oder mit SnapManager das Backup wiederherstellen und ein anderes Tool wie Oracle Recovery Manager (RMAN) zur Wiederherstellung der Daten verwenden. Da SnapManager die Backups mit RMAN registrieren kann, können Sie die Datenbank mit feineren Besonderheiten wie Blöcken wiederherstellen. Diese Integration vereint die Geschwindigkeit und die Speichereffizienz von Snapshot-Kopien mit der feinen Steuerung für die Wiederherstellung mit RMAN.

Sie müssen eine Datenbank wiederherstellen, bevor Sie sie verwenden können. Sie können jedes beliebige Werkzeug oder Skript verwenden, um eine Datenbank wiederherzustellen.

Ab SnapManager 3.2 für Oracle ermöglicht SnapManager die automatische Wiederherstellung von Datenbank-Backups mithilfe der Archiv-Log-Backups. Selbst wenn die Archiv-Log-Backups am externen Standort zur Verfügung stehen, verwendet SnapManager die Archiv-Log-Backups vom externen Standort zum Wiederherstellen der Datenbank-Backups.

Wenn der Datenbank neue Datendateien hinzugefügt werden, empfiehlt Oracle, sofort ein neues Backup zu erstellen. Wenn Sie außerdem ein Backup wiederherstellen, das vor dem Hinzufügen der neuen Datendateien erstellt wurde, und versuchen Sie, es nach dem Hinzufügen der neuen Datendateien zu einem Punkt wiederherzustellen, kann der automatische Oracle-Wiederherstellungsprozess fehlschlagen, da es keine Datendateien erstellen kann. In der Oracle-Dokumentation finden Sie Informationen zum Prozess zur Wiederherstellung von Datendateien, die nach einem Backup hinzugefügt wurden.

Für den Wiederherstellungsprozess benötigter Datenbankstatus

Der Status der Datenbank, die wiederhergestellt werden soll, hängt von der Art des Wiederherstellungsprozesses, die Sie durchführen möchten, und der Art der Dateien ab, die enthalten sein sollen.

In der folgenden Tabelle ist der Status aufgeführt, in dem die Datenbank von der ausgewählten Wiederherstellungsoption und dem Typ der Dateien abhängig sein soll, die in die Wiederherstellung aufgenommen werden sollen:

Art der Wiederherstellung	Enthaltene Dateien	Datenbankstatus für diese Instanz	Datenbank-Status für andere Instanz (nur RAC)
Nur Restore	Kontrolldateien	Herunterfahren	Herunterfahren
Systemdateien	Montieren oder herunterfahren	Montieren oder herunterfahren	Keine Systemdateien
Alle Bundesstaaten	Alle Bundesstaaten	Restore und Recovery	Kontrolldateien
Herunterfahren	Herunterfahren	Systemdateien	Montieren

Art der Wiederherstellung	Enthaltene Dateien	Datenbankstatus für diese Instanz	Datenbank-Status für andere Instanz (nur RAC)
Montieren oder herunterfahren	Keine Systemdateien	Mount oder Offen	Alle

Der von SnapManager für einen Wiederherstellungsvorgang erforderliche Datenbankzustand ist von dem ausgeführten Wiederherstellungstyp abhängig (vollständige, partielle oder Kontrolldateien). SnapManager übergibt die Datenbank nicht in einen niedrigeren Zustand (z. B. von Öffnen auf Mount), es sei denn, die Force-Option ist angegeben.

Die Pläne für die Vorschau der Wiederherstellung sind

SnapManager bietet Wiederherstellungspläne vor und nach Abschluss des Wiederherstellungsvorgangs. Mit den Wiederherstellungsplänen werden verschiedene Wiederherstellungsmethoden in der Vorschau, Prüfung und Analyse angezeigt.

Struktur des Wiederherstellungsplans

Der Wiederherstellungsplan besteht aus den folgenden beiden Abschnitten:

- Vorschau/Prüfung: Dieser Abschnitt beschreibt, wie SnapManager jede Datei wiederherstellen (oder wiederherstellen hat).
- Analyse: Dieser Abschnitt beschreibt, warum einige Wiederherstellungsmechanismen während des Wiederherstellungsvorgangs nicht verwendet wurden.

Der Abschnitt Vorschau/Überprüfung

In diesem Abschnitt wird gezeigt, wie jede Datei wiederhergestellt wird oder wiederhergestellt wurde. Wenn Sie den Wiederherstellungsplan vor einem Wiederherstellungsvorgang anzeigen, wird er als Vorschau bezeichnet. Wenn Sie sie nach Abschluss eines Wiederherstellungsvorgangs anzeigen, wird sie als Überprüfung bezeichnet.

Das folgende Vorschaubeispiel zeigt, dass die Dateien mit einer schnellen Volume-basierten Wiederherstellung, einer speicherseitigen Filesystem-Wiederherstellung und einer Storage-seitigen Systemwiederherstellung wiederhergestellt werden. Um festzustellen, warum alle Dateien nicht mit derselben Wiederherstellungsmethode wiederhergestellt werden würden, lesen Sie den Abschnitt Analyse.

```
Preview:
The following files will be restored completely via: fast restore
+DG1/rac6/users.dbf

The following files will be restored completely via: storage side file
system restore
+DG2/rac6/sysaux.dbf
+DG2/rac6/system.dbf
The following files will be restored completely via: storage side system
restore
+DG2/rac6/undotbs1.dbf
+DG2/rac6/undotbs2.dbf
```

Jede Wiederherstellungsmethode hat einen Unterabschnitt, der Informationen über die Dateien enthält, die mit dieser Wiederherstellungsmethode wiederhergestellt werden können. Die Unterabschnitte werden nach abnehmenden Niveaus der Lagermethodeneffizienz geordnet. Im Beispiel oben ist die schnelle Wiederherstellungsmethode effizienter als die Wiederherstellungsmethode des Speicherdateisystems und wird daher zuerst angezeigt.

Es ist möglich, dass eine Datei durch mehrere Wiederherstellungsmethoden wiederhergestellt werden kann. Mehrere Wiederherstellungsmethoden werden verwendet, wenn die für ein Filesystem verwendeten LUNs (Logical Unit Numbers) auf verschiedene Storage-System-Volumes verteilt werden und einige Volumes für die Volume-Wiederherstellung infrage kommen, andere hingegen nicht. Wenn mehrere Wiederherstellungsmethoden verwendet werden, um dieselbe Datei wiederherzustellen, wird der Vorschaubereich wie folgt angezeigt:

```
The following files will be restored via a combination of:
[fast restore, storage side file system restore. storage side system
restore]
```

Der Abschnitt Analyse

Der Abschnitt Analyse enthält die Gründe, warum einige Wiederherstellungsmechanismen nicht oder wurden nicht verwendet. Anhand dieser Informationen können Sie ermitteln, welche Daten benötigt werden, um effizientere Restore-Mechanismen zu ermöglichen.

Das folgende Beispiel zeigt einen Abschnitt „Analyse“:

```
Analysis:

The following reasons prevent certain files from being
restored completely via: fast restore
   * LUNs present in snapshot of volume fas960:
        /vol/rac_6_asm_disks may not be consistent when reverted:
        [fas960:/vol/rac6_asm_disks/DG4D1.lun]
     Mapped LUNs in volume fas960:/vol/rac_6_asm_disks
        not part of the restore scope will be reverted: [DG4D1.lun]

Files to restore:
     +DG2/rac6/sysaux.dbf
     +DG2/rac6/system.dbf
     +DG2/rac6/undotbs1.dbf
     +DG2/rac6/undotbs2.dbf

* Reasons denoted with an asterisk (*) are overridable.
```

Im Beispiel ist der erste Fehler übersteuerbar durch die Verwendung von -fast -override von der Befehlszeilenschnittstelle (CLI) oder durch die Auswahl von **Override** in der grafischen Benutzeroberfläche (GUI). Der zweite Fehler über zugeordnete LUNs im Volume ist obligatorisch und nicht zu überrätselfähig.

Sie können die Prüfungen wie folgt beheben:

- Um einen obligatorischen Prüffehler zu beheben, ändern Sie die Umgebung, damit die Prüfung erfolgreich ist.
- Um einen übersteuerbaren Prüffehler zu beheben, können Sie die Umgebung ändern oder die Prüfung überschreiben.

  Sie müssen jedoch vorsichtig sein, da das Überschreiben der Prüfung zu unerwünschten Folgen führen kann.

Anzeigen der Informationen zur Wiederherstellung von Backups in der Vorschau

Sie können vorab eine Vorschau der Informationen zu einem Backup-Wiederherstellungsprozess anzeigen, um Informationen über die Berechtigung zur Wiederherstellung zu erhalten, die SnapManager für Oracle auf Ihrem Backup gefunden hat. SnapManager analysiert die Daten für Ihr Backup, um festzustellen, ob der Wiederherstellungsprozess erfolgreich abgeschlossen werden kann.

Die Vorschau zur Wiederherstellung enthält die folgenden Informationen:

- Über den welcher Restore-Mechanismus (schnelle Wiederherstellung, Storage-seitige Filesystem-Wiederherstellung, Storage-seitige Datei-Wiederherstellung oder Host-seitige Datei-Kopie-Wiederherstellung) kann jede Datei wiederhergestellt werden.
- Warum effizientere Mechanismen nicht für die Wiederherstellung jeder Datei verwendet wurden, wenn Sie die -verbose Option angeben.

Wenn Sie im Befehl Backup Restore die Option-Preview angeben, stellt SnapManager nichts wieder her, listet aber die wiederherzustellenden Dateien auf und gibt an, wie sie wiederhergestellt werden.

Sie können alle Arten von Wiederherstellungsmechanismen in einer Vorschau anzeigen. Die Vorschau zeigt Informationen über bis zu 20 Dateien.

1. Geben Sie den folgenden Befehl ein:smo Backup restore -profileprofile_Name-labellabel-complete -Preview -verbose

   Geben Sie beispielsweise Folgendes ein:

   ```
   smo backup restore -profile targetdb1_prof1
         -label full_bkup_sales_nov_08  -complete -preview -verbose
   ```

   Das folgende Beispiel zeigt einige Dateien, die mit dem Host-seitigen Dateikopierprozess wiederhergestellt werden, und erklärt auch, warum einige Dateien mit der Option fast Restore nicht wiederhergestellt werden können. Wenn Sie die Option -verbose angeben, zeigt SnapManager einen Vorschaubereich und einen Analysebereich an, der erläutert, warum jede Datei nicht über den schnellen Wiederherstellungsprozess wiederhergestellt werden kann.

```
PREVIEW:
The following files will be restored via host side file copy restore:
+DG2/sid/datafile10.dbf
+DG2/sid/datafile11.dbf

ANALYSIS:
The following reasons prevent certain files from being restored via fast
restore:
Reasons:
 Newer snapshots of /vol/volume2 have volume clones: SNAP_1
*Newer backups will be freed: nightly2, nightly3
Files to Restore:
/mnt/systemB/volume2/system.dbf
/mnt/systemB/volume2/users.dbf
/mnt/systemB/volume2/sysaux.dbf
/mnt/systemB/volume2/datafile04.dbf
/mnt/systemB/volume2/datafile05.dbf

The following reasons prevent certain files from being restored via fast
restore:
Reasons:
* Newer snapshots of /vol/adm_disks will be lost: ADM_SNAP_5
* Luns present which were created after snapshot SNAP_0 was created:
/vol/adm_disks/disk5.lun
* Files not part of the restore scope will be reverted in file system:
+DG2

Files Not in Restore Scope: +DG2/someothersid/data01.dbf
+DG2/someothersid/data02.dbf
Files to Restore:
+DG2/sid/datafile08.dbf +DG2/sid/datafile09.dbf
+DG2/sid/datafile10.dbf +DG2/sid/datafile11.dbf

* Reasons denoted with an asterisk (*) are overridable.
```

2. Prüfen Sie die Gründe, warum andere Wiederherstellungsprozesse nicht verwendet werden können.
3. Starten Sie den Wiederherstellungsvorgang ohne die Option -Preview, wenn nur Gründe angezeigt werden, die überschreibbar sind.

   Sie können nicht obligatorische Prüfungen weiterhin überschreiben.

Wiederherstellung von Backups mit schneller Wiederherstellung

Sie können SnapManager für Oracle dazu zwingen, den Volume-basierten SnapRestore-Prozess anstelle anderer Restore-Prozesse zu verwenden, wenn alle obligatorischen

Bedingungen für die schnelle Wiederherstellung erfüllt werden.

Sie können den Befehl Backup Restore mit -fast verwenden: `backup restore -fast [require | override | fallback | off]`

Sie können die Option -fast nur verwenden, wenn Sie eine vollständige Wiederherstellung eines vollständigen Backups durchführen möchten. Die Option -fast umfasst die folgenden Parameter:

- Erforderlich: Ermöglicht die Wiederherstellung eines Volumes, wenn alle obligatorischen Bedingungen für die Wiederherstellung erfüllt sind und keine überrückbaren Prüfungen gefunden werden.

  Wenn Sie die Option -fast angeben, jedoch keinen Parameter für -fast angeben, verwendet SnapManager als Standard den Parameter-erfordern.

- Überschreiben: Ermöglicht Ihnen, nicht obligatorische Eignungsprüfungen zu überschreiben und die Volume-basierte schnelle Wiederherstellung durchzuführen.
- Fallback: Ermöglicht es Ihnen, die Datenbank mit jeder Methode wiederherzustellen, die SnapManager bestimmt.

  Wenn Sie nicht -fast angeben, verwendet SnapManager den Parameter -Fallback als Standard.

- Aus: Sie können die Zeit, die für die Durchführung aller Eignungsprüfungen erforderlich ist, vermeiden, um einen dateibasierten Wiederherstellungsprozess anstelle des schnellen Wiederherstellungsprozesses durchzuführen.

Wenn das Backup die obligatorischen Eignungsprüfungen nicht bestanden hat, kann die schnelle Wiederherstellung nicht erfolgreich abgeschlossen werden.

SnapManager führt ausschließlich Volume-basierte schnelle Restores in UNIX-basierten Umgebungen durch. SnapManager führt in der Windows-Umgebung keine schnellen Restores durch.

Während VBSR auf der Datensicherung der Datendatei ausgeführt wird, wenn die Datendateien und die Archivprotokolldateien im selben Volume vorhanden sind und wenn die Archivprotokolldateien nicht im aktiven Dateisystem vorhanden sind, ist die Wiederherstellung und Wiederherstellung der Datenbank erfolgreich. Die zukünftigen Archiv-Log-Snapshots werden jedoch als Teil der VBSR gelöscht, was zu einem veralteten Eintrag des Archiv-Log-Backups im Repository führt.

1. Geben Sie den folgenden Befehl ein:smo Backup restore -profileprofile_Name-labellabel-complete-fast requkurz-wortrecih

   ```
   smo backup restore -profile targetdb1_prof1
         -label full_bkup_sales_nov_08  -complete -fast require -verbose
   ```

2. Prüfen Sie die Prüfungen der Berechtigung zur schnellen Wiederherstellung.
3. Wenn die Eignungsprüfung feststellt, dass keine obligatorischen Prüfungen fehlgeschlagen sind, wenn bestimmte Bedingungen überschrieben werden können und wenn Sie mit dem Wiederherstellungsprozess fortfahren möchten, geben Sie den folgenden Befehl ein: Backup restore -fast override

Verwandte Informationen

Erstellen von vor-, Post-Task- und Richtlinienskripten

Variablen, die in den Taskskripten für den Wiederherstellungsvorgang verfügbar sind

Speichern der Taskskripte

Wiederherstellen von Backups mithilfe von Single File SnapRestore

Sie können die Backups mithilfe der Single File SnapRestore-Methode (SFSR) wiederherstellen.

1. Erstellen Sie ein Profil über die grafische Benutzeroberfläche von SnapManager (GUI).
2. Sichern Sie die Datenbank mithilfe der GUI.
3. Heben Sie die Verknüpfung der Service-Gruppen für Oracle und Network File System (NFS) von den Cluster-Service-Gruppen auf und frieren Sie sie ein.
4. Stellen Sie sicher, dass die Secure Shell (SSH) zwischen den Hosts und SnapDrive für UNIX konfiguriert ist, indem Sie in der Datei snapdrive.conf #Secure-Communication-between-Cluster-Nodes auf ON setzen.
5. Führen Sie über die Benutzeroberfläche von SnapManager vollständige Backup-Restores und -Recovery mit --Alllogs durch.
6. Heben Sie das Einfrieren der Service-Gruppen auf und verknüpfen Sie sie zurück mit der Cluster-Service-Gruppe.

   Diese Konfiguration ist nur anwendbar, wenn Sie SnapDrive 4.1.1 D2 für UNIX und SnapDrive 4.2 für UNIX verwenden.

   Wenn einem Wiederherstellungsvorgang ein anderer Wiederherstellungsvorgang gefolgt wird, besteht die Möglichkeit, dass die Erstellung der Snapshot Kopie des Backups fehlschlägt. Wenn Sie sukzessive Wiederherstellungsvorgänge innerhalb der angegebenen Zeit ausführen, in der der SFSR abgeschlossen werden kann, tritt bei SnapManager für Oracle ein Erstellungsfehler der Snapshot Kopie auf.

   Um Fehler beim Erstellen von Snapshot Kopien zu vermeiden, stellen Sie sicher, dass Restore-Vorgänge nach dem Zeitraum durchgeführt werden, in dem SFSR ausgeführt wird.

   Überprüfen Sie dazu den Status des Split-Prozesses für LUN-Klone, indem Sie den folgenden Befehl aus der Befehlszeilenschnittstelle (CLI) des Storage-Systems eingeben: Rshfilernnamelun Clone Split statuslun-Name

   ```
   Sample Output:
   /vol/delaware_760gb/lun700gb (64% complete)..
   ```

   Volume-basiertes SnapRestore (VBSR) wird nicht auf Solaris Hosts mit Veritas Stack mit SFRAC- und VCS-Umgebung unterstützt.

Wiederherstellung von Backups auf dem Primärspeicher

Sie können mit dem Befehl Backup Restore ein Datenbank-Backup im Primärspeicher wiederherstellen.

SnapManager versucht standardmäßig eine Volume-basierte, schnelle Wiederherstellung durchzuführen und bietet Informationen zur Überprüfung der Berechtigung. Sie können bei Bedarf einige Eignungsüberprüfungen

überschreiben. Wenn Sie sicher sind, dass ein Backup nicht mithilfe einer schnellen Wiederherstellung durchgeführt werden kann, können Sie die Prüfung der Berechtigung zur schnellen Wiederherstellung deaktivieren und eine dateibasierte Wiederherstellung durchführen.

Mithilfe der Befehlsoptionen für die Backup-Wiederherstellung können Sie angeben, ob SnapManager den gesamten oder einen Teil des Backups wiederherstellen soll. Mit SnapManager können Sie außerdem Kontrolldateien zusammen mit den Datendateien oder Tablespaces aus den Backups in einem einzelnen Benutzervorgang wiederherstellen. Sie können -controlfiles mit -Complete integrieren, um Kontrolldateien zusammen mit Tabellen und Datendateien wiederherzustellen.

Sie können eine der folgenden Optionen zur Wiederherstellung des Backups auswählen:

Sie möchten wiederherstellen…	**Verwenden…**
Das gesamte Backup mit allen Tabellen und Datendateien	-Abgeschlossen
Die Liste bestimmter Tabellen	-Tabellen
Bestimmte Datendateien	-Dateien
Nur die Kontrolldateien	-Controlfiles
Tablespaces, Datendateien und Kontrolldateien	-Complete -controlfiles

Sie können das Backup auch von einem alternativen Speicherort wiederherstellen, indem Sie -restorespec angeben.

Wenn Sie -Recovery einschließen, können Sie die Datenbank wiederherstellen, um:

- Zur letzten Transaktion, die in der Datenbank durchgeführt wurde (alle Logs)
- Zu einem bestimmten Datum und einer bestimmten Uhrzeit
- Eine bestimmte Oracle Systemänderungsnummer (SCN)
- Zum Zeitpunkt des Backups (keine Protokolle)
- Nur Restore

Sowohl die Datums- als auch die Zeitwiederherstellung sowie die SCN-Wiederherstellung sind Point-in-Time Recovery.

SnapManager (3.2 oder höher) bietet die Möglichkeit, die wiederhergestellten Datenbank-Backups automatisch mithilfe der Archivprotokolldateien wiederherzustellen. Selbst wenn die Archivprotokolldateien am externen Speicherort verfügbar sind, wenn Sie die Option -recover-from-location angeben, verwendet SnapManager die Archivprotokolldateien vom externen Speicherort, um die wiederhergestellten Datenbank-Backups wiederherzustellen.

SnapManager stellt Oracle den externen Standort zur Verfügung. Aber Oracle erkennt die Dateien vom externen Ziel nicht. Dieses Verhalten wird bei der Bestimmung des Flash-Recovery-Bereichs und beim ASM-Ziel (Automatic Storage Management) festgestellt. Dies sind Probleme mit Oracle und die Problemumgehung besteht darin, immer eine Sicherung von Archiv-Log-Dateien in solchen Datenbank-Layouts zu haben.

Wenn ein inkonsistentes SCN oder Datum angegeben wird, wird die Wiederherstellung am letzten konsistenten Punkt, der mit der Fehlermeldung Wiederherstellung erfolgreich, aber nicht ausreichend beendet. Die Wiederherstellung muss manuell in einen konsistenten Zustand erfolgen.

Für eine Wiederherstellung, wenn keine Protokolle angewendet werden, stellt SnapManager bis zum letzten SCN der letzten während des Backups erstellten Archivprotokolldatei wieder her. Wenn die Datenbank konsistent ist bis zu diesem SCN, dann wird die Datenbank erfolgreich geöffnet. Wenn die Datenbank zu diesem Zeitpunkt nicht konsistent ist, versucht SnapManager immer noch, die Datenbank zu öffnen, die erfolgreich geöffnet wird, wenn die Datenbank bereits konsistent ist.

SnapManager unterstützt nicht die Wiederherstellung der ausschließlich Archiv-Log-Backups.

Wenn das Archivprotokoll auf einem NFS-Mount-Punkt nicht Snapshot-fähiger Storage ist, können Sie mit SnapManager die wiederhergestellten Datenbank-Backups mithilfe des Profils wiederherstellen. Bevor Sie SnapManager-Vorgänge auf einem nicht-Snapshot-fähigen Storage durchführen, sollten Sie die Ziele für archivedLogs.exclude in smo.config hinzufügen.

Sie müssen sicherstellen, dass Sie den Parameter Ausschließen festlegen, bevor Sie ein Profil erstellen. Erst nachdem der Parameter exclude in der SnapManager-Konfigurationsdatei festgelegt wurde, ist die Profilerstellung erfolgreich.

Wenn die Datenbank ein nicht-Snapshot-fähiger Speicher auf einer ASM-Laufwerksgruppe ist und wenn die Datenbank als Archiv-Protokollziel ausgewählt wird, unterstützt SnapManager die Wiederherstellung der Backups mit dem Profil nicht.

Wenn das Backup bereits angehängt ist, mounted SnapManager den Backup nicht erneut und verwendet das bereits bereitgestellte Backup. Wenn das Backup von einem anderen Benutzer gemountet wird und der aktuelle Benutzer keinen Zugriff auf das zuvor bereitgestellte Backup hat, müssen andere Benutzer die Berechtigungen bereitstellen. Alle Archivprotokolldateien haben Leseberechtigungen für die Gruppen-Eigentümer; der aktuelle Benutzer hat möglicherweise nicht die Berechtigungen, wenn das Backup von einer anderen Benutzergruppe gemountet wird. Die Benutzer können Berechtigungen für die gemounteten Archivprotokolldateien manuell erteilen und die Wiederherstellung oder Wiederherstellung wiederholen.

Wiederherstellung von Datenbank-Backups in einer RAC-Umgebung (Real Application Clusters

Während der Wiederherstellung der Datenbank-Backups in einer RAC-Umgebung, wenn die erforderliche Archivprotokolldatei nicht gefunden wird, Oracle Anfragen für Archiv-Log-Dateien und Schalter zwischen verschiedenen Threads und Änderungsnummer in der RAC-Datenbank. SnapManager für Oracle versucht, die Datenbank als besten Aufwand wiederherzustellen. Das erfolgreiche Recovery der Datenbank-Backups in der RAC-Umgebung hängt von der Verfügbarkeit der Archiv-Log-Dateien in den Backups ab.

Der empfohlene Wiederherstellungsmechanismus für die RAC-Datenbank ist wie folgt:

- Stellen Sie sicher, dass alle Archivprotokolldateien in den Backups oder alle Archivprotokolldateien im einen externen Archivprotokollziel verfügbar sind.
- Wenn mehrere externe Archiv-Protokollziele bereitgestellt werden, können Sie Überschneidungen der Archiv-Log-Dateien bereitstellen, während Sie die externen Archiv-Protokollziele für alle Threads angeben.

  Zum Beispiel, die externe Archiv-Log-Speicherort - Ich kann 1 bis 100 Archiv-Log-Dateien, die externe Archiv-Log-Speicherort - II haben können 98 bis 200 Archiv-Log-Dateien, und die externe Archiv-Log-Speicherort - III kann 198 bis 300 Archiv-Log-Dateien haben.

- Beim Beschneiden der Archivprotokolldateien können Sie die Archiv-Log-Dateien bis zu SCN oder Datum löschen, sodass die Backups dieselben Archivprotokolldateien haben können.

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen Wiederherstellungsvorgang zu sammeln.

1. Geben Sie den folgenden Befehl ein:smo Backup restore -profile_Name-Label-complete-recover -alllogs [-recover-from-locationpath [,path2]]-dump-verbose

   smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 - complete -restore -alllogs -wortrecih

2. Um Daten für verschiedene Szenarien wiederherzustellen, führen Sie einen der folgenden Schritte aus:

Sie möchten wiederherstellen…	**Befehlsbeispiel**
Vollständige Datenbank ohne Kontrolldateien und Wiederherstellung auf eine bestimmte SCN-Nummer (3794392). In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber alle Datendateien sind beschädigt oder verloren. Stellen Sie die Datenbank von einem bestehenden vollständigen Online-Backup auf einen Punkt unmittelbar vor diesem SCN. wieder her	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -Recovery -bis 3794392 -verbose
Komplette Datenbank ohne Kontrolldateien und Wiederherstellung bis zu einem Datum und einer Uhrzeit.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -Recovery -until 2008-09-15:15:29:23 -verbose
Komplette Datenbank ohne Kontrolldateien und Wiederherstellung bis zu einer Daten und Zeit. In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber alle Datendateien sind beschädigt oder verloren oder ein logischer Fehler trat nach einer bestimmten Zeit auf. Stellen Sie die Datenbank von einem bestehenden kompletten Online-Backup auf ein Datum und eine Uhrzeit unmittelbar vor dem Fehlerpunkt wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -Recovery -bis „2008-09-15:15:29:23“ -verbose
Partielle Datenbank (eine oder mehrere Datendateien) ohne Kontrolldateien und wiederherstellen mit allen verfügbaren Protokollen. In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber eine oder mehrere Datendateien sind beschädigt oder verloren. Stellen Sie diese Dateien wieder her und stellen Sie die Datenbank von einem bestehenden vollständigen Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -files /u02/oradata/sales02.dbf /u02/oradata/sale03.dbf /u02/oradata/sale04.dbf -restore -alllogs -verbose

Sie möchten wiederherstellen…	Befehlsbeispiel
Partielle Datenbank (ein oder mehrere Tabellen) ohne Kontrolldateien und Recovery mit allen verfügbaren Protokollen. In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber ein oder mehrere Tabellen werden verworfen oder eine von mehreren Datendateien, die zu dem Tablespace gehören, ist beschädigt oder verloren. Stellen Sie diese Tabellen wieder her und stellen Sie die Datenbank aus einem vorhandenen kompletten Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -Tablespaces Users -Recovery -alllogs -verbose
Nur Steuern Dateien und erholen mit allen verfügbaren Protokollen. In diesem Fall existieren die Datendateien, aber alle Kontrolldateien sind beschädigt oder verloren. Stellen Sie nur die Steuerdateien wieder her und stellen Sie die Datenbank aus einem bestehenden vollständigen Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -controlfiles -Recovery -alllogs -verbose
Vollständige Datenbank ohne Kontrolldateien und Wiederherstellung mit den Backup-Kontrolldateien und allen verfügbaren Protokollen. In diesem Fall sind alle Datendateien beschädigt oder verloren gegangen. Stellen Sie nur die Steuerdateien wieder her und stellen Sie die Datenbank aus einem bestehenden vollständigen Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -using-Backup -controlfile -recover -alllogs -wortrecih
Wiederherstellen der wiederhergestellten Datenbank mit den Archiv-Log-Dateien aus dem externen Archiv-Log-Speicherort.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -using-Backup -controlfile -Recovery -alllogs -recover-from-location /user1/Archive -verbose

3. Prüfen Sie die Prüfungen der Berechtigung zur schnellen Wiederherstellung.

   Geben Sie den folgenden Befehl ein: smo Backup restore -profile targetdb1_prof1 -Label full_bkup_Sales_nov_08 -complete -recover -alllogs -recover-from-location /user1/Archive -verbose

4. Wenn in der Eignungsprüfung angezeigt wird, dass keine obligatorischen Prüfungen fehlgeschlagen sind und bestimmte Bedingungen außer Kraft gesetzt werden können, und wenn Sie mit dem Wiederherstellungsprozess fortfahren möchten, geben Sie Folgendes ein: Backup restore -fast override
5. Geben Sie mithilfe der Option -recover-from-location externe Archivprotokolle an.

Verwandte Informationen

Wiederherstellung von Backups mit schneller Wiederherstellung

Wiederherstellen von Backups von einem alternativen Speicherort

Der Smo Backup Restore Befehl

Durchführen von Recovery auf Blockebene mit Oracle Recovery Manager (RMAN)

Sie können SnapManager für den Katalog seiner Backups im Recovery Manager (RMAN), einem Oracle Tool, konfigurieren, damit Sie mithilfe von RMAN ein Recovery auf Blockebene durchführen können. RMAN kann die Kontrolldateien der Datenbank oder eine separate Recovery-Katalog-Datenbank als Repository verwenden.

1. Geben Sie den folgenden Befehl ein, um eine vollständige Offline-Sicherung mithilfe von SnapManager durchzuführen:

   smo Backup create -offline-full-profilprofile_Name-labelBackup_Label_Name-wortrecih

   Wo?

   - Profile_Name ist der Name des Profils, das der Sicherung zugeordnet ist
   - Backup_Label_Name ist der Name des Backup-Labels

```
smo backup create -offline -full -profile profile_monthly
-label full_backup -verbose

+
SMO-07109 [INFO ]: Cataloguing all files in backup set with RMAN
TAG=SMC_full_backup_1158773581857, RMAN=ES0/controlfile.
...
SMO-13037 [INFO ]: Successfully completed operation: Backup
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:02:20.506
Operation Id [ff8080810dcc47e3010dcc47eb7a0001] succeeded.
+
```

1. Um zu überprüfen, ob das Backup mit RMAN katalogisiert ist, geben Sie vom Datenbank-Host den folgenden Befehl an der RMAN-Eingabeaufforderung ein:

   Liste datafilecopy Tag Tag Tag_Name;

```
RMAN> list datafilecopy tag SMO_full_backup_1158773581857;

Recovery Manager: Release 10.2.0.1.0 - Production on Wed Sep 20 10:33:41
2008
Copyright (c) 1982, 2008, Oracle. All rights reserved.
using target database control file instead of recovery catalog
 List of Datafile Copies
 Key File S Completion Time Ckp SCN Ckp Time Name
 ------- ---- - --------------- ---------- --------------- ---
 335 1 A 20-SEP-08 1347825 20-SEP-08
 /opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
 /system01.dbf
 336 2 A 20-SEP-08 1347825 20-SEP-08
 /opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
 /undotbs01.dbf
 334 3 A 20-SEP-08 1347825 20-SEP-08
 /opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
 /sysaux01.dbf
 333 4 A 20-SEP-08 1347825 20-SEP-08
 /opt/<path>/smo/mnt/Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47e3010dcc47e
b7a0001
 /user01.dbf
 337 5 A 20-SEP-08 1347825 20-SEP-08
 RMAN>
```

2. Geben Sie den folgenden Befehl ein, um die Datenbank zu überprüfen und festzustellen, ob Blöcke beschädigt sind:

   dbv-DATEI=user01.dbf

   Die folgende Ausgabe gibt an, dass zwei Seiten beschädigt sind:

```
DBVERIFY: Release 10.2.0.1.0 - Production on Wed Sep 20 13:35:44 2006
Copyright (c) 1982, 2005, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = user01.dbf
Page 625 is marked corrupt
Corrupt block relative dba: 0x01400271 (file 5, block 625)
Bad header found during dbv:
Data in bad block:
type: 240 format: 6 rdba: 0xed323b81
last change scn: 0x6f07.faa74628 seq: 0x87 flg: 0x02
spare1: 0x60 spare2: 0x5 spare3: 0xef7d
consistency value in tail: 0xa210fe71
check value in block header: 0x13c7
block checksum disabled...
Page 627 is marked corrupt
Corrupt block relative dba: 0x01400273 (file 5, block 627)
Bad header found during dbv:
Data in bad block:
type: 158 format: 7 rdba: 0x2101e16d
last change scn: 0xe828.42414628 seq: 0xb4 flg: 0xff
spare1: 0xcc spare2: 0x81 spare3: 0x8665
consistency value in tail: 0x46d20601
check value in block header: 0x1a84
computed block checksum: 0x6c30
DBVERIFY - Verification complete
Total Pages Examined : 1280
Total Pages Processed (Data) : 1123
Total Pages Failing (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing (Index): 0
Total Pages Processed (Other): 34
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
Total Pages Empty : 120
Total Pages Marked Corrupt: 2
Total Pages Influx : 0
Highest block SCN : 1337349 (0.1337349)
```

3. Um den Zugriff auf die Dateien vom Backup auf den Host und RMAN zu ermöglichen, mounten Sie das Backup mit dem folgenden Befehl:

   smo Backup Mount -profileprofile_Name-labellabel-verbose

```
smo backup mount -profile SALES1 -label full_backup -verbose

SMO-13046 [INFO ]: Operation GUID 8abc013111b9088e0111b908a7560001
starting on Profile SALES1
SMO-08052 [INFO ]: Beginning to connect mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/logs from
snapshot SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_logs.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/logs from
snapshot SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_logs.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/data from
snapshot SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_data.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/data from
snapshot SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_data.
SMO-08053 [INFO ]: Finished connecting mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001.
SMO-13037 [INFO ]: Successfully completed operation: Backup Mount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:01:00.981
Operation Id [8abc013111b9088e0111b908a7560001] succeeded.
```

4. Geben Sie zum Wiederherstellen der Blöcke in RMAN den folgenden Befehl ein:

   Blockrecover-Datendatei '/Mountpoint/path/file.dbf' Block Block_id, vom Tag Backup_rman_Tag

```
RMAN> blockrecover datafile
‘/mnt/ssys1/Host4_ES0/file01.dbf’ block 625, 626, 627
from tag SMO_full_backup_1158773581857;

Starting blockrecover at 20-SEP-08 using target database control file
instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=153 devtype=DISK
channel ORA_DISK_1: restoring block(s) from datafile copy
 /opt/NetApp/smo/mnt/_mnt_ssys1_Host4_ES0_SMO_E_ES0_F_C_0_ff8080810dcc47
e3010dcc47eb7a0001/user01.dbf
starting media recovery
media recovery complete, elapsed time: 00:00:01
Finished blockrecover at 20-SEP-08
```

5. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die Blöcke repariert wurden:

   dbv-DATEI=filename.dbf

   Die folgende Ausgabe zeigt an, dass keine Seiten beschädigt sind:

```
dbv FILE=user01.dbf

DBVERIFY: Release 10.2.0.1.0 - Production on Wed Sep 20 13:40:01 2008
Copyright (c) 1982, 2008, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = user01.dbf
DBVERIFY - Verification complete
Total Pages Examined : 1280
Total Pages Processed (Data) : 1126
Total Pages Failing (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing (Index): 0
Total Pages Processed (Other): 34
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
Total Pages Empty : 120
Total Pages Marked Corrupt : 0
Total Pages Influx : 0
Highest block SCN : 1337349 (0.1337349)
```

   Alle beschädigten Blöcke wurden repariert und wiederhergestellt.

Wiederherstellung von Dateien aus einem anderen Speicherort

SnapManager ermöglicht Ihnen, Datendateien von einem anderen Speicherort als die

von Snapshot Kopien im ursprünglichen Volume wiederherzustellen und zu kontrollieren.

Der ursprüngliche Speicherort ist der Speicherort der Datei auf dem aktiven Dateisystem zum Zeitpunkt des Backups. Der alternative Speicherort ist der Speicherort, von dem eine Datei wiederhergestellt wird.

Sie können folgende Daten von einem alternativen Speicherort wiederherstellen:

- Die Datendateien von einem Zwischendateisystem zu einem aktiven Dateisystem
- Die Datenblöcke von einem Zwischenrohgerät zu einem aktiven Rohgerät

Die Recovery wird durch SnapManager automatisiert. Bei der Wiederherstellung von Dateien von externen Speicherorten verwendet SnapManager den Befehl „Wiederherstellung automatisch von Standort aus“.

SnapManager setzt für die Wiederherstellung von Dateien auch den Oracle Recovery Manager (RMAN) ein. Die wiederherzustellenden Dateien sollten von Oracle erkennbar sein. Die Dateinamen sollten im Standardformat vorliegen. Bei der Wiederherstellung aus einem Flash-Recovery-Bereich liefert SnapManager den übersetzten Weg zu Oracle. Oracle ist jedoch nicht aus dem Flash-Recovery-Bereich wiederhergestellt, da es nicht den richtigen Dateinamen generieren kann. Idealerweise sollte der Flash-Recovery-Bereich als Ziel mit RMAN genutzt werden.

Verwandte Informationen

Erstellen von Wiederherstellungsspezifikationen

Stellen Sie Backups aus einer Übersicht über einen alternativen Speicherort wieder her

Verwenden Sie zum Wiederherstellen eines Datenbank-Backups von einem anderen Standort die folgenden wichtigen Schritte, die jeweils weiter in diesem Abschnitt beschrieben werden.

- Führen Sie je nach Datenbank-Layout einen der folgenden Schritte aus:
  - Stellen Sie die erforderlichen Datendateien von Band, SnapVault, SnapMirror oder anderen Medien auf jedem beliebigen Filesystem wieder her, das auf dem Datenbank-Host gemountet ist.
  - Stellen Sie das erforderliche Dateisystem wieder her und mounten Sie es auf dem Datenbank-Host.
  - Stellen Sie eine Verbindung zu den erforderlichen RAW-Geräten her, die im lokalen Host vorhanden sind.
- Erstellen Sie eine XML-Datei (Extensible Markup Language) für die Wiederherstellungsspezifikation, die die Zuordnungen enthält, die SnapManager vom alternativen Speicherort zum ursprünglichen Speicherort wiederherstellen muss. Speichern Sie die Datei an einem Speicherort, auf den SnapManager zugreifen kann.
- Verwenden Sie SnapManager, um die Daten mithilfe der XML-Datei für die Wiederherstellungsspezifikation wiederherzustellen und wiederherzustellen.

Wiederherstellung der Daten aus Dateien

Bevor Sie ein Restore von einem alternativen Speicherort aus durchführen, müssen Sie die erforderlichen Dateien von einem beliebigen Storage-Medium wiederherstellen und die Dateien von Applikationen wie SnapVault oder SnapMirror in einem Dateisystem wiederherstellen, das auf dem lokalen Host gemountet ist.

Sie können die Wiederherstellung aus einem alternativen Speicherort verwenden, um die Dateien von einem

alternativen Dateisystem auf ein aktives Dateisystem zu kopieren.

Sie müssen die alternativen Speicherorte angeben, von denen die Originaldateien wiederhergestellt werden sollen, indem Sie eine Wiederherstellungsspezifikation erstellen.

Wiederherstellung von Daten aus dem Dateisystem

Bevor Sie Daten von einem alternativen Speicherort wiederherstellen, müssen Sie das erforderliche Filesystem wiederherstellen und es auf dem lokalen Host mounten.

Sie können den Wiederherstellungsvorgang von einem alternativen Speicherort aufrufen, um die Dateien von alternativen Dateisystemen auf aktive Dateisysteme zu kopieren.

Um diesen Vorgang durchzuführen, müssen Sie die alternativen Mount-Punkte angeben, von denen die ursprünglichen Mount-Punkte und die Namen der ursprünglichen Snapshot-Kopie wiederhergestellt werden sollen, indem Sie eine Spezifikationsdatei für die Wiederherstellung erstellen.

Der Name der Snapshot Kopie ist eine erforderliche Komponente, da dasselbe Filesystem mehrmals in einer einzelnen Backup-Operation gesichert werden kann (z. B. einmal für die Datendateien und einmal für die Log-Datei).

Für das automatische Speichermanagement (ASM) muss der Name der Laufwerksgruppe mit der Laufwerksgruppe übereinstimmen, die SnapManager geklont hat, um das Backup mit Oracle Recovery Manager (RMAN) zu registrieren. Dieser Name kann durch Anzeigen der Backup-Eigenschaften abgerufen werden.

Verwandte Informationen

Erstellen von Wiederherstellungsspezifikationen

Wiederherstellung der Daten von RAW-Geräten

Bevor Sie ein anderes Verzeichnis wiederherstellen, müssen Sie eine Verbindung zu den auf dem lokalen Host vorhandenen Raw-Geräten herstellen.

Sie können die Wiederherstellung von einem alternativen Speicherort aufrufen, um die Datenblöcke von alternativen Rohgeräten auf aktive Raw Devices zu kopieren. Um diesen Vorgang durchzuführen, müssen Sie das alternative RAW-Gerät angeben, von dem aus das ursprüngliche RAW-Gerät wiederhergestellt werden soll, indem Sie eine Wiederherstellungsspezifikation erstellen.

Verwandte Informationen

Erstellen von Wiederherstellungsspezifikationen

Erstellen von Wiederherstellungsspezifikationen

Die Spezifikationsdatei für die Wiederherstellung ist eine XML-Datei, die die ursprünglichen und alternativen Speicherorte enthält, aus denen die Datei wiederhergestellt werden kann. SnapManager verwendet diese Spezifikationsdatei, um Dateien vom angegebenen Speicherort wiederherzustellen.

Sie können die Wiederherstellungsspezifikationsdatei mit einem beliebigen Texteditor erstellen. Sie müssen eine .XML-Erweiterung für die Datei verwenden.

1. Öffnen Sie eine Textdatei.
2. Geben Sie Folgendes ein: <restore-Specification xmlns="" class="bare">http://www.netapp.com">
3. Geben Sie alle Informationen zur Dateizuordnung unter Verwendung des im folgenden Beispiel gezeigten Formats ein:

```
<file-mapping>
    <original-location>/path/dbfilename.dbf</original-location>
    <alternate-location>/path/dbfilename1.dbf</alternate-location>
</file-mapping>
```

   Die Dateizuordnung gibt an, aus welcher Datei wiederhergestellt wird. Der ursprüngliche Speicherort ist der Speicherort der Datei auf dem aktiven Dateisystem zum Zeitpunkt der Sicherung. Der alternative Speicherort ist der Speicherort, von dem die Datei wiederhergestellt wird.

4. Geben Sie alle Informationen zur Dateisystemzuordnung unter Verwendung des im Beispiel gezeigten Formats ein:

```
<mountpoint-mapping>
     <original-location>/path/db_name</original-location>
     <snapname>snapname</snapname>
     <alternate-location>/path/vaultlocation</alternate-location>
</mountpoint-mapping>
<mountpoint-mapping>
     <original-location>+DiskGroup_1</original-location>
     <snapname>snapname</snapname>
     <alternate-location>+DiskGroup_2</alternate-location>
</mountpoint-mapping>
```

   Mountpunkt bezieht sich auf Verzeichnispfad /mnt/myfs/)oder auf einen Bereitstellungspunkt für die Datenträgergruppe Automatic Storage Management (ASM) (zum Beispiel +MY_DG). Die Mountpunkt-Mapping-Zuordnung gibt den Bereitstellungspunkt an, aus dem die Dateien wiederhergestellt werden. Der ursprüngliche Speicherort ist der Speicherort des Mountpoint im aktiven File-System zum Zeitpunkt des Backups. Der alternative Speicherort ist der Bereitstellungspunkt, aus dem die Dateien im ursprünglichen Speicherort wiederhergestellt werden. Der Snapname ist der Name der Snapshot Kopie, in der die Originaldateien gesichert wurden.

   Bei ASM muss der Name der Laufwerksgruppe mit der Laufwerksgruppe übereinstimmen, die SnapManager für die Registrierung des Backups mit RMAN geklont hat. Dieser Name kann durch Anzeigen der Backup-Eigenschaften abgerufen werden.

   > Der Name einer Snapshot Kopie ist eine notwendige Komponente, da dasselbe Filesystem in einem einzelnen Backup-Vorgang mehrfach eingesetzt werden kann (z. B. einmal für die Datendateien und einmal für die Protokolle).

5. Geben Sie die Tags und Standorte für die RAW-Gerätezuordnung mithilfe des im Beispiel gezeigten Formats ein:

```
<raw-device-mapping>
     <original-location>/path/raw_device_name</original-location>
     <alternate-location>/path/raw_device_name</alternate-location>
</raw-device-mapping>
```

RAW Device Mapping gibt den Speicherort an, von dem ein RAW-Gerät wiederhergestellt wird.

6. Geben Sie Folgendes ein: </Restore-Specification>
7. Speichern Sie die Datei als .XML-Datei und schließen Sie die Spezifikation.

Beispiel für die Wiederherstellung der Spezifikation

Das folgende Beispiel zeigt die Struktur der wiederherstellenden Spezifikationen:

```
<?xml version="1.0" encoding="UTF-8"?>
<restore-specification xmlns="http://www.netapp.com">
<!-- "Restore from file(s)" -->
     <file-mapping>
          <original-location>/mnt/pathname/dbname/users01.dbf</original-
location>
          <alternate-location>/mnt/vault/users01.dbf</alternate-location>
     </file-mapping>
<!-- "Restore from host mounted file system(s)" -->
     <mountpoint-mapping>
          <original-location>/mnt/pathname/dbname/fs</original-location>
          <snapname>Snapshotname</snapname>
          <alternate-location>/mnt/vaultlocation</alternate-location>
     </mountpoint-mapping>
<!-- "Restore from ASM mounted file system(s)" -->
     <mountpoint-mapping>
          <original-location>+DISKGROUP_1</original-location>
          <snapname>snapshotname</snapname>
          <alternate-location>+DISKGROUP_2</alternate-location>
     </mountpoint-mapping>
<!-- "Restore from raw device" -->
     <raw-device-mapping>
          <original-location>/pathname/devicename</original-location>
          <alternate-location>/pathname/devicename</alternate-location>
     </raw-device-mapping>
</restore-specification>
```

Wiederherstellen von Backups von einem alternativen Speicherort

Sie können Backups von einem alternativen Speicherort wiederherstellen, um die Datendateien von einem zwischengeschalteten Dateisystem in ein aktives Dateisystem

wiederherzustellen oder die Datenblöcke von einem Zwischenrohgerät in ein aktives RAW-Gerät wiederherzustellen.

- Erstellen Sie eine XML-Datei für die Wiederherstellungsspezifikation, und geben Sie den Typ der Wiederherstellungsmethode an, die Sie verwenden möchten.

Sie können den Befehl smo Backup restore verwenden und die XML-Datei für die Wiederherstellungsspezifikation angeben, die Sie erstellt haben, um das Backup von einem anderen Speicherort wiederherzustellen.

1. Geben Sie den folgenden Befehl ein: smo Backup restore -profilprofile-labellabel-complete-alllogs -restorespecrestorespec

Verwandte Informationen

Der Smo Backup Restore Befehl

Klonen der Datenbank-Backup

Wenn Sie eine Datenbank klonen, können Sie Aufgaben wie das Testen eines Upgrades auf eine Datenbank durchführen, ohne die produktive Datenbank zu beeinträchtigen, eine Master-Installation auf mehrere Trainingssysteme zu duplizieren oder eine Master-Installation als Basisinstallation auf andere Server mit ähnlichen Anforderungen zu duplizieren.

Sie können die folgenden Aufgaben zum Klonen ausführen:

- Klonen einer Datenbank aus einem vorhandenen Backup
- Klonen einer Datenbank im aktuellen Status, mit der Sie das Backup und den Klon in einem Verfahren erstellen können.
- Klonen eines geschützten Backups auf dem sekundären oder gar tertiären Storage
- Klonen Sie eine Datenbank und verwenden Sie benutzerdefinierte Plug-in-Skripte, die vor oder nach dem Klonvorgang ausgeführt werden.
- Klonen einer Datenbank auf demselben Host, auf dem sich die Datenbank befindet.
- Klonen einer Datenbank unter Verwendung von Archivprotokolldateien aus dem externen Archivprotokoll.
- Klonen einer Datenbank auf einem alternativen Host
- Klonen einer RAC-Datenbank.
- Zeigen Sie eine Liste von Klonen an.
- Anzeigen von detaillierten Kloninformationen
- Klone löschen

Klonen

Sie können eine Datenbank klonen, um ein exaktes Replikat der Originaldatenbank zu erstellen. Sie können den Klon von einem vollständigen Backup oder vom aktuellen Status der Datenbank aus erstellen.

Zum Erstellen eines Klons mit SnapManager gehören folgende Vorteile:

Vorteile	Details
Schnell	Der Klonvorgang bei SnapManager nutzt die in Data ONTAP verfügbare FlexClone Funktion. Somit können Sie große Datenvolumen schnell klonen.
Platzeffizienz	Wenn Sie einen Klon mit SnapManager erstellen, wird Speicherplatz nur für die Änderungen zwischen dem Backup und dem Klon benötigt. Ein SnapManager-Klon ist eine beschreibbare Snapshot Kopie der Originaldatenbank und kann nach Bedarf erweitert werden. Hingegen erfordert ein physischer Klon der Datenbank, dass Ihnen genügend Speicherplatz zum Kopieren der gesamten Datenbank zur Verfügung steht.
Virtuelle Kopie	Sie können die geklonte Datenbank so verwenden, als wäre sie die ursprüngliche Datenbank. Beispielsweise können Sie einen Klon für Tests, Überprüfungen von Plattformen und Updates, Mehrfachsimulationen mit großen Datenmengen und Tests und Probeläufe an Remote Standorten verwenden. Änderungen am Klon haben keine Auswirkung auf die ursprüngliche Datenbank. Nachdem die Datenbank geklont wurde, ist die geklonte Datenbank vollständig betriebsbereit.
Einfachheit	Sie können eine Datenbank mithilfe von SnapManager Befehlen auf einem beliebigen Host klonen.

Sie können ein Backup auf dem primären (lokalen) Storage oder einem geschützten Backup auf dem sekundären (Remote) Storage klonen. Ein Backup kann jedoch nicht geklont werden, wenn der Backup-Vorgang ausgeführt wird oder das Backup auf den sekundären Storage übertragen wurde.

Sie müssen sicherstellen, dass die folgenden Voraussetzungen erfüllt sind, bevor eine Datenbank geklont werden kann:

- Stellen Sie sicher, dass das Verzeichnis [/etc/var/opt/oracle]/oratab keinen Eintrag enthält, der auf die Kennung des Zielsystems verweist.
- Löschen Sie die Datei sfile<SID>.ora aus €ORACLE_HOME/dbs.
- Löschen Sie die Datei init<SID>.ora aus €Oracle_HOME/dbs.
- Löschen Sie die Oracle Dump-Ziele, die in der Klon-Spezifikations-Datei angegeben sind.
- Löschen Sie die Oracle-Steuerdateien, die in der Klon-Spezifikations-Datei angegeben sind.
- Löschen Sie die Oracle Redo-Protokolldateien, die in der Klon-Spezifikations-Datei angegeben sind.

Sie müssen dem Klon eine neue Systemkennung geben. Sie können nicht gleichzeitig zwei Datenbanken mit derselben Systemkennung auf demselben Host ausführen. Sie können einen Klon auf einem anderen Host mit

der gleichen Systemkennung erstellen. Sie können den Klon entweder mit einer Bezeichnung versehen oder SnapManager eine Bezeichnung erstellen lassen. Dazu verwenden Sie die Systemkennung, das Datum und die Uhrzeit der Klonerstellung.

Wenn Sie ein Etikett eingeben, dürfen Sie keine Leerzeichen oder Sonderzeichen enthalten.

Im Rahmen des Klonprozesses erstellt SnapManager die nötigen Oracle Dateien und Parameter für die geklonte Datenbank. Ein Beispiel für eine notwendige Oracle-Datei ist init<SID>.ora.

Wenn Sie eine Datenbank klonen, erstellt SnapManager im Verzeichnis Oracle_HOME/dbs eine neue init<SID>.ora-Datei für die Datenbank.

Wenn SnapManager den Storage für eine Datenbank klonen, erstellt es auch einen neuen Filesystem-Bereitstellungspunkt, ändert aber nicht die Verzeichnisstruktur unter dem Bereitstellungspunkt aus der SnapManager CLI. In der SnapManager GUI können Sie jedoch die Verzeichnisstruktur und die Metadaten des Dateisystems ändern.

Oracle 11g in einer Direct NFS-Umgebung (DNFS) ermöglicht eine zusätzliche Mountpoint-Konfiguration, wie z. B. mehrere Pfade für den Lastausgleich in der oranfstab-Datei. SnapManager ändert diese Datei nicht. Daher müssen nach dem Klonen mit SnapManager alle weiteren Eigenschaften, die ein Klon verwenden soll, manuell der oranfstab-Datei hinzugefügt werden.

Sie können eine RAC-Datenbank (Real Application Cluster) sowie eine nicht-Cluster-Datenbank klonen. Ein RAC-Klon wird als einzige Datenbank gestartet.

Sie können ein Datenbank-Backup auf dem Host, auf dem sich die Datenbank befindet, oder auf einem alternativen Host klonen.

Sie können eine ASM-Datenbank auch auf einem Remote-Host klonen. Wenn Sie dies tun, müssen Sie sicherstellen, dass die ASM-Instanz auf dem Remote-Host ausgeführt wird.

Wenn die geklonte Datenbank eine spfile verwendet, erstellt SnapManager eine spfile für den Klon. Diese Datei wird in das Verzeichnis „€Oracle_HOME/dbs“ gespeichert und erstellt die Verzeichnisstruktur für die Diagnosedateien. Der Dateiname ist sfile <SID>.ora.

Klonmethoden

Sie können eine Datenbank mit einer von zwei Methoden klonen. Die von Ihnen gewählte Methode wirkt sich auf den Erstellungsvorgang des Klons aus.

In der folgenden Tabelle werden die Klonmethoden und ihre Auswirkung auf den Vorgang zum Erstellen von Klonen und seine Option -Reserve beschrieben. Eine LUN kann mit beiden Methoden geklont werden.

Klonmethode
Beschreibung
Clone create -Reserve
Klonen von LUNs
Es wird eine neue Klon-LUN innerhalb desselben Volumes erstellt.

Klonmethode
Wenn -Reserve für eine LUN auf „yes“ eingestellt ist, ist der Speicherplatz für die volle LUN-Größe innerhalb des Volume reserviert.
Klonen von Volumes
Es wird ein neuer FlexClone erstellt und die Klon-LUN innerhalb des neuen Klon-Volume vorhanden ist. Verwendet FlexClone Technologie.
Wenn -Reserve für ein Volume auf „ja“ eingestellt ist, ist der Speicherplatz für die volle Volume-Größe innerhalb des Aggregats reserviert.

Erstellen von Klonspezifikationen

SnapManager für Oracle verwendet eine XML-Datei für die Klonspezifikation, die die Zuordnungen, Optionen und Parameter für die Verwendung im Klonvorgang umfasst. SnapManager verwendet diese Informationen, um zu bestimmen, wo die von ihm klonen und wie mit Diagnosedaten, Kontrolldateien, Parametern usw. umzugehen ist.

Sie können die Klon-Spezifikationsdatei über die grafische Benutzeroberfläche von SnapManager (GUI), die Befehlszeilenschnittstelle (CLI) oder einen Texteditor erstellen.

Wenn Sie die Clone Specification-Datei mithilfe eines Texteditors erstellen, müssen Sie sie als XML-Datei speichern. Sie können diese XML-Datei für andere Klonvorgänge verwenden.

Sie können auch eine Vorlage für Klonspezifikationen erstellen und diese dann anpassen. Sie können den Befehl „smo Clone template“ oder in der GUI verwenden, den Clone Wizard verwenden.

SnapManager für Oracle fügt einer beliebigen Klon-Spezifikations-Vorlage, die sie erstellt, einen Versionsstring hinzu. SnapManager für Oracle geht von der neuesten Version für jede Klon-Spezifikations-Datei aus, die keinen Versionsstring enthält.

Wenn Sie Remote-Klone durchführen möchten, ändern Sie in der Klonspezifikationsdatei nicht die Standardorte der Datendateien, Wiederherstellungsprotokolle und Kontrolldateien. Wenn Sie den Standardspeicherort ändern, erstellt SnapManager nicht den Klon oder erstellt den Klon für einer Datenbank, die keine Snapshot-Funktion unterstützt. Daher schlägt die automatische Profilerstellung fehl.

Obwohl Mount-Punkt- und ASM-Datenträgergruppen-Informationen über die GUI editierbar sind, können Sie nur den Dateinamen und nicht die Dateiorte ändern.

Sie können eine Aufgabe mehrfach ausführen, entweder mit den gleichen oder mit unterschiedlichen Parameter- und Wertkombinationen.

1. Öffnen Sie eine Textdatei und geben Sie Text ein, wie im folgenden Beispiel gezeigt:

```
<clone-specification xmlns="http://www.example.com>
     <storage-specification/>
     <database-specification/>
 </clone-specification>
```

2. Geben Sie in der Komponente Speicherspezifikation die Bereitstellungspunkte für die Datendateien ein.

   In der Storage-Spezifikation werden die Speicherorte für den für den Klon erstellten neuen Storage aufgeführt, wie z. B. Mount-Punkte für Datendateien und Rohgeräte. Diese Elemente müssen vom Quell- dem Ziel zugeordnet werden.

   Im folgenden Beispiel wird die Syntax für den Mount-Punkt der Datendatei angezeigt, die Sie in der Klonspezifikation verwenden:

```
<mountpoint>
     <source>/mnt/path/source_data file_mountpoint</source>
     <destination>/mnt/path/target_data file_mountpoint</destination>
</mountpoint>
```

3. Optional: Wenn Sie ein RAW-Gerät auf der Quelle haben, müssen Sie den Pfad für das RAW-Gerät auf der Quelle angeben und dann das Ziel automatisch generieren=`"true`" für das Ziel angeben.

   Anders als in der Clone Mapping-Datei von früheren Versionen von SnapManager für Oracle können Sie keinen Speicherort für das RAW-Gerät auf dem Ziel angeben. SnapManager für Oracle wählt den nächsten verfügbaren Gerätenamen für das geklonte RAW-Gerät aus.

   Im folgenden Beispiel wird die Syntax der RAW-Geräte angezeigt, die Sie in der Klonspezifikation verwenden:

```
<raw-device>
     <source>/dev/raw/raw1</source>
     <destination auto-generate="true"/>
</raw-device>
```

4. Geben Sie in der Komponente Datenbankspezifikation die Informationen der Steuerdatei als eine Liste der Steuerdateien an, die Sie für den Klon erstellen möchten.

   Die Datenbankspezifikation gibt die Datenbankoptionen für den Klon an, z. B. Kontrolldateien, Wiederherstellungsprotokolle, Archivprotokolle und Oracle Parameter.

   Im folgenden Beispiel wird die Syntax der Kontrolldatei angezeigt, die Sie in der Klonspezifikation verwenden:

```
<controlfiles>
     <file>/mnt/path/clonename/control/control01.ctl</file>
     <file>/mnt/path/clonename/control/control02.ctl</file>
</controlfiles>
```

5. Geben Sie die Struktur des Wiederherstellungsprotokolls für den Klon an.

   Im folgenden Beispiel wird die Struktur des Wiederherstellungsprotokollverzeichnisses für das Klonen angezeigt:

```
<redologs>
     <redogroup>
          <file>/mnt/path/clonename/redo/redo01.log</file>
          <number>1</number>
          <size unit="M">100</size>
     </redogroup>
     <redogroup>
         <file>/mnt/path/clonename/redo/redo02.log</file>
         <number>2</number>
         <size unit="M">100</size>
     </redogroup>
</redologs>
```

6. Geben Sie die Oracle-Parameter an, die in der geklonten Datenbank auf unterschiedliche Werte festgelegt werden sollen. Wenn Sie Oracle 10 verwenden, müssen Sie die folgenden Parameter angeben:
   - Hintergrundauszug
   - Core Dump
   - User Dump
   - (Optional) Archivprotokolle

   > Wenn die Parameterwerte nicht richtig festgelegt sind, wird der Klonvorgang angehalten, und Sie erhalten eine Fehlermeldung.

   Wenn Sie nicht den Speicherort der Archivprotokolle angeben, erstellt SnapManager den Klon im Noarchivelog Modus. SnapManager kopiert diese Parameterinformationen in die init.ora-Datei des Klons.

   + im folgenden Beispiel wird die Parametersyntax angezeigt, die Sie in der Klonspezifikation verwenden:

```
<parameters>
     <parameter>
          <name>log_archive_dest_1</name>
          <value>LOCATION=/mnt/path/clonename/archive</value>
     </parameter>
</parameters>
```

+ + Sie können einen Standardwert verwenden, indem Sie ein Standardelement innerhalb des Parameterelements verwenden. Im folgenden Beispiel übernimmt der Parameter os_Authentication_PREFIX den Standardwert, da das Standardelement angegeben wird:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <default></default>
     </parameter>
</parameters>
```

+ + Sie können einen leeren String als Wert für einen Parameter mithilfe eines leeren Elements angeben. Im folgenden Beispiel wird das os_Authentication_PREFIX auf einen leeren String gesetzt:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <value></value>
     </parameter>
</parameters>
```

+ + HINWEIS: Sie können den Wert aus der init.ora-Datei der Quelldatenbank für den Parameter verwenden, indem Sie kein Element angeben.

+ + Wenn ein Parameter mehrere Werte hat, können Sie die durch Kommas getrennten Parameterwerte angeben. Wenn Sie beispielsweise die Datendateien von einem Ort in einen anderen verschieben möchten, können Sie den Parameter db_file_Name_convert verwenden und die durch Kommas getrennten Datendateipfade angeben, wie im folgenden Beispiel zu sehen ist:

+

+

+

```
<parameters>
     <parameter>
          <name>db_file_name_convert</name>
          <value>>/mnt/path/clonename/data file1,/mnt/path/clonename/data
file2</value>
     </parameter>
</parameters>
```

+ + Wenn Sie die Protokolldateien von einem Ort in einen anderen verschieben möchten, können Sie im Folgenden den Parameter log_file_Name_convert verwenden und die durch Kommas getrennten Protokolldateipfade angeben, wie im Beispiel zu sehen:

+

+

+

```
<parameters>
     <parameter>
          <name>log_file_name_convert</name>

<value>>/mnt/path/clonename/archivle1,/mnt/path/clonename/archivle2</value
>
     </parameter>
</parameters>
```

1. Optional: Geben Sie beliebige SQL-Anweisungen an, die für den Klon ausgeführt werden sollen, wenn er online ist.

   Sie können die SQL-Anweisungen verwenden, um Aufgaben auszuführen, wie z. B. das Neuerstellen der temporären Dateien in der geklonten Datenbank.

   Sie müssen sicherstellen, dass am Ende der SQL-Anweisung kein Semikolon enthalten ist.

   Im Folgenden finden Sie eine Beispiel-SQL-Anweisung, die Sie im Rahmen des Klonvorgangs ausführen:

```
<sql-statements>
   <sql-statement>
     ALTER TABLESPACE TEMP ADD
     TEMPFILE '/mnt/path/clonename/temp_user01.dbf'
     SIZE 41943040 REUSE AUTOEXTEND ON NEXT 655360
     MAXSIZE 32767M
   </sql-statement>
</sql-statements>
```

Beispiel für Klonspezifikation

Im folgenden Beispiel wird die Klonspezifikationsstruktur angezeigt, die sowohl die Komponenten für die Storage- als auch die Datenbankspezifikation enthält:

```
<clone-specification xmlns="http://www.example.com>

   <storage-specification>
     <storage-mapping>
        <mountpoint>
          <source>/mnt/path/source_mountpoint</source>
          <destination>/mnt/path/target_mountpoint</destination>
        </mountpoint>
        <raw-device>
          <source>/dev/raw/raw1</source>
          <destination auto-generate="true"/>
        </raw-device>
        <raw-device>
          <source>/dev/raw/raw2</source>
          <destination auto-generate="true"/>
        </raw-device>
     </storage-mapping>
   </storage-specification>

   <database-specification>
     <controlfiles>
       <file>/mnt/path/clonename/control/control01.ctl</file>
       <file>/mnt/path/clonename/control/control02.ctl</file>
     </controlfiles>
     <redologs>
         <redogroup>
           <file>/mnt/path/clonename/redo/redo01.log</file>
           <number>1</number>
           <size unit="M">100</size>
        </redogroup>
        <redogroup>
```

```
            <file>/mnt/path/clonename/redo/redo02.log</file>
            <number>2</number>
            <size unit="M">100</size>
          </redogroup>
      </redologs>
      <parameters>
        <parameter>
          <name>log_archive_dest_1</name>
          <value>LOCATION=/mnt/path/clonename/archive</value>
        </parameter>
        <parameter>
          <name>background_dump_dest</name>
          <value>/mnt/path/clonename/admin/bdump</value>
        </parameter>
        <parameter>
          <name>core_dump_dest</name>
          <value>/mnt/path/clonename/admin/cdump</value>
        </parameter>
        <parameter>
          <name>user_dump_dest</name>
          <value>/mnt/path/clonename/admin/udump</value>
        </parameter>
      </parameters>
    </database-specification>
</clone-specification>
```

Verwandte Informationen

Klonen von Datenbanken und mit benutzerdefinierten Plug-in-Skripten

Klonen von Datenbanken aus Backups

Das Klonen von Datenbanken im aktuellen Status

Überlegungen beim Klonen einer Datenbank auf einem alternativen Host

Klonen von Datenbanken und mit benutzerdefinierten Plug-in-Skripten

SnapManager bietet eine Methode zum Verwenden der benutzerdefinierten Skripte vor und nach einem Klonvorgang. Beispielsweise haben Sie vielleicht ein benutzerdefiniertes Skript erstellt, das eine Klon-Datenbank-SID validiert und sicherstellt, dass die SID von Ihrer Benennungsrichtlinie zulässig ist. Mit dem SnapManager Klon-Plug-in können Sie Ihre benutzerdefinierten Skripts einschließen und sie automatisch vor oder nach einem SnapManager Klonvorgang ausführen lassen.

1. Zeigen Sie Beispielskripts für das Plug-in an.
2. Erstellen Sie ein Skript von Grund auf, oder ändern Sie eines der Beispielskripts für das Plug-in.

Erstellen Sie Ihr benutzerdefiniertes Skript gemäß den Richtlinien des SnapManager Plug-in-Skripts.

3. Legen Sie Ihr benutzerdefiniertes Skript an einen bestimmten Speicherort für das Verzeichnis.
4. Aktualisieren Sie die XML-Datei für die Klonspezifikation und fügen Sie Informationen zu Ihrem benutzerdefinierten Skript ein, das während des Klonens verwendet werden soll.
5. Überprüfen Sie mit einem SnapManager-Befehl, ob die benutzerdefinierten Skripts betriebsbereit sind.
6. Geben Sie beim Starten des Klonvorgangs den Namen des Skripts und optionale Parameter an.

Klonen von Datenbanken aus Backups

Sie können eine Datenbank aus einer Sicherung klonen, indem Sie den Befehl „Clone create“ verwenden.

Sie müssen zuerst eine Klon-Spezifikations-Datei für die Datenbank erstellen. SnapManager erstellt den Klon auf der Grundlage der Informationen in dieser Spezifikationsdatei.

Sie müssen dem Klon eine neue Oracle System Identifier (SID) geben. Sie können nicht zwei Datenbanken mit derselben SID gleichzeitig auf dem gleichen Host ausführen. Sie können einen Klon auf einem anderen Host haben, der dieselbe SID verwendet. Um einen eindeutigen Namen für den Klon festzulegen, verwenden Sie -Label. Falls Sie diese Option nicht verwenden, erstellt SnapManager einen eindeutigen Namen für den Klon, der SID, Datum und Uhrzeit enthält.

Nachdem Sie eine Datenbank geklont haben, sollten Sie Ihre nsnames.ora-Dateien auf Ihren Clientcomputern mit den neuen geklonten Datenbankverbindungsinformationen aktualisieren. Die tnsnames.ora-Dateien werden verwendet, um eine Verbindung zu einer Oracle-Instanz herzustellen, ohne die vollständigen Datenbankinformationen angeben zu müssen. SnapManager aktualisiert die Dateien nsnames.ora nicht.

SnapManager erstellt immer eine Sicherung einschließlich Archivprotokolldateien, wenn Sie das mit -include -with-Online-Backups erstellte Profil verwenden. SnapManager ermöglicht Ihnen das Klonen nur der vollständigen Datenbank-Backups.

SnapManager (3.2 oder höher) ermöglicht Ihnen, die Backups zu klonen, die die Datendateien und archivierte Log-Dateien enthalten.

Wenn das Archivprotokoll von einem externen Standort aus verfügbar ist, können Sie beim Klonen den externen Standort angeben, um die geklonte Datenbank in einen konsistenten Status wiederherzustellen. Sie müssen sicherstellen, dass Oracle auf den externen Speicherort zugreifen kann. Das Klonen der rein archivprotokollbasierten Backups wird nicht unterstützt.

Obwohl das Backup des Archivprotokolls zusammen mit dem Online-Backup eines partiellen Backups erstellt wird, können Sie mit diesem Backup keinen Datenbankklon erstellen.

Sie können die Datenbanksicherung vom Speicherort der externen Archivprotokolldatei nur für eine eigenständige Datenbank klonen.

Das Klonen der Online-Datenbanksicherung der RAC-Datenbank (Real Application Clusters) unter Verwendung des Speicherorts für externe Archivprotokolldateien schlägt aufgrund eines Fehlers bei der Wiederherstellung fehl. Dies liegt daran, dass die Oracle Datenbank während des Klonens des Datenbank-Backups die Archivprotokolldateien nicht für die Recovery vom externen Speicherort des Archivierungsprotokolls findet und wendet sie an.

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen Klonvorgang zu sammeln.

Datendatei-Backup ohne Archiv-Log-Backup klonen

Wenn die Datensicherung der Datendateien nicht das Backup des Archivprotokolls umfasst, klont SnapManager für Oracle die Datenbank auf Basis der während des Backups aufgezeichneten Systemänderungsnummer (SCN). Wenn die geklonte Datenbank nicht wiederhergestellt werden kann, wird die für die Fertigstellung der Wiederherstellung erforderliche archivierte Protokolldatei für Thread <number> und Change <SCN> angezeigt, obwohl SnapManager für Oracle die Datenbank weiterhin klont und den Klon schließlich erfolgreich erstellt.

Beim Klonen unter Verwendung der Datendateien Backup ohne Einbindung des Archivprotokolls stellt SnapManager die geklonte Datenbank bis zum letzten Archivprotokoll-SCN wieder her, das während des Backups aufgezeichnet wird.

1. Erstellen einer Clone Specification File.
2. Um einen Klon zu erstellen, geben Sie den folgenden Befehl ein: smo Clone create -Backup -labelBackup_Name-newsidneft_sid-labelclone_Label-profilprofile_Name -clonespepfull_path_to_clonespepfile [-taskspectaskundspecspecSpec] [-recover-from-location] path1 [,<path2>…][-dump]

Verwandte Informationen

Das Klonen von Datenbanken im aktuellen Status

Überlegungen beim Klonen einer Datenbank auf einem alternativen Host

Erstellen von Klonspezifikationen

Der Befehl Smo Clone create

Erstellen von vor-, Post-Task- und Richtlinienskripten

In den Aufgabenskripten verfügbare Variablen für den Klonvorgang

Aufgabenskripte werden erstellt

Speichern der Taskskripte

Das Klonen von Datenbanken im aktuellen Status

Sie können mit einem einzigen Befehl ein Backup und einen Klon der Datenbank aus dem aktuellen Status der Datenbank erstellen.

Wenn Sie das Profil mit der Option -current angeben, erstellt SnapManager zuerst ein Backup und dann einen Klon im aktuellen Status der Datenbank.

Wenn Sie in der Profileinstellung das Backup von Datendateien und Archivprotokollen zum Klonen zusammen aktiviert haben, werden bei jedem Backup der Online-Datendateien auch die Archivprotokolle gesichert. Während des Klonens der Datenbank erstellt SnapManager das Backup der Datendateien zusammen mit dem Archivprotokoll-Backup und erstellt den Datenbankklon. Wenn die Backup des Archivprotokolls nicht enthalten ist, erstellt SnapManager nicht das Backup des Archivprotokolls und kann daher nicht den Klon der Datenbank erstellen.

1. Um die Datenbank im aktuellen Status zu klonen, geben Sie den folgenden Befehl ein: smo Clone create -profilprofile_Name-current -labelclonepec./clonespec_filename.xml

Dieser Befehl erstellt sofort ein vollständiges automatisches Backup (das Backup-Label generiert) und erstellt anhand einer vorhandenen Klonspezifikation einen Klon aus diesem Backup.

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach den erfolgreichen oder fehlgeschlagenen Vorgängen zu sammeln. Der Dump wird sowohl für die Backup- als auch für Klonvorgänge erfasst.

Klonen von Datenbank-Backups ohne Umsetzungsprotokolle

SnapManager ermöglicht Ihnen ein flexibles Klonen, sodass Sie die geklonte Datenbank manuell bis zu einem gewünschten Zeitpunkt wiederherstellen können, ohne die Datenbank über ResetLogs zu öffnen. Sie können die geklonte Datenbank auch manuell als Data Guard Standby-Datenbank konfigurieren.

Wenn Sie die Option -no-resetlogs beim Erstellen des Klons auswählen können, führt SnapManager die folgenden Aktivitäten aus, um die geklonte Datenbank zu erstellen:

1. Führt die Vorverarbeitung, falls angegeben, vor dem Start des Klonvorgangs aus
2. Erstellt die geklonte Datenbank mit der vom Benutzer angegebenen SID
3. Führt die SQL-Anweisungen aus, die für die geklonte Datenbank ausgegeben wurden.

   Nur die SQL-Anweisungen, die im Mount-Status ausgeführt werden können, wurden erfolgreich ausgeführt.

4. Führt die Aktivität der Aufgabe nach der Verarbeitung aus, falls angegeben.

Welche Aufgaben müssen Sie tun, um die geklonte Datenbank manuell wiederherzustellen

1. Mounten Sie die Archiv-Log-Backups und stellen Sie die geklonte Datenbank manuell wieder her, indem Sie die Archiv-Log-Dateien vom gemounteten Pfad verwenden.
2. Öffnen Sie nach der Durchführung manueller Wiederherstellung die wiederhergestellte geklonte Datenbank mit der Option -Resetlogs.
3. Erstellen Sie bei Bedarf temporäre Tablespaces.
4. Führen Sie das DBNEWID-Dienstprogramm aus.
5. Gewähren sie den Anmeldeinformationen der geklonten Datenbank sysdba-Berechtigung.

Beim Klonen der Datenbank-Backups mit der Option -no-resetlogs lässt SnapManager die geklonte Datenbank im gemounteten Status zur manuellen Wiederherstellung zurück.

Die mit der Option -no-resetlogs erstellte geklonte Datenbank ist keine vollständige Datenbank. Daher dürfen Sie SnapManager Operationen auf dieser Datenbank nicht ausführen, obwohl SnapManager Sie nicht daran hindert, irgendwelche Operationen auszuführen.

Wenn Sie die Option -no-resetlogs nicht angeben, wendet SnapManager die Archiv-Log-Dateien an und öffnet die Datenbank mit Resetlogs.

1. Geben Sie den folgenden Befehl ein: smo Clone create -profilprofile_Name [-Backup-labelbackup_Name in den folgenden Fällen: -Backup-idBackup_id current] -newsidneft_sid-clonespepfull_path_to_clonespepfile -no-resetlogs

Wenn Sie versuchen, sowohl -no-resetlogs als auch Recovery-from-location Optionen anzugeben, erlaubt SnapManager nicht, diese beiden Optionen zusammen anzugeben, und zeigt die Fehlermeldung an: SMO-04084: Sie müssen entweder eine der Optionen angeben: -No-resetlogs oder -Recovery-from-location.

Beispiel

```
smo clone create -profile product -backup-label full_offline -newsid
PROD_CLONE -clonespec prod_clonespec.xml -label prod_clone-reserve -no
-reset-logs
```

Überlegungen beim Klonen einer Datenbank auf einem alternativen Host

Bevor Sie auf einem anderen Host als dem Klon der Datenbank klonen können, müssen einige Anforderungen erfüllt werden.

Folgende Tabelle zeigt die Setup-Anforderungen für Quell- und Zielhost:

Vorbedingung eingerichtet	Anforderungen
Der Netapp Architektur Sind	Muss auf den Quell- und Ziel-Hosts identisch sein
Betriebssystem und Version	Muss auf den Quell- und Ziel-Hosts identisch sein
SnapManager für Oracle	Muss auf den Quell- und Ziel-Hosts installiert und ausgeführt werden
Anmeldedaten	Muss festgelegt werden, damit der Benutzer auf den Zielhost zugreifen kann
Oracle	Die Software-Version muss auf den Quell- und Ziel-Hosts installiert sein. Der Oracle-Listener muss auf dem Ziel-Host ausgeführt werden.
Kompatibler Storage Stack	Muss auf den Quell- und Ziel-Hosts identisch sein
Protokoll für den Zugriff auf Datendateien	Muss auf den Quell- und Ziel-Hosts identisch sein
Volumenmanager	Die Konfiguration muss sowohl auf den Quell- als auch auf den Ziel-Hosts erfolgen und von kompatiblen Versionen sein

Sie können auch eine ASM-Datenbank (Automatic Storage Management) auf einem Remote-Host klonen. Wenn Sie dies tun, müssen Sie sicherstellen, dass die ASM-Instanz auf dem Remote-Host ausgeführt wird.

Klonen einer Datenbank auf einem alternativen Host

Sie können mit dem Befehl Clone create ein Datenbank-Backup auf einem alternativen Host klonen.

- Erstellen Sie ein Profil oder haben Sie ein vorhandenes Profil.
- Erstellen Sie ein vollständiges Backup oder ein bereits vorhandenes Datenbank-Backup.
- Erstellen Sie eine Klonspezifikation oder weisen Sie eine vorhandene Klonspezifikation auf.
  a. Geben Sie zum Klonen einer Datenbank auf einem anderen Host den folgenden Befehl ein: smo Clone create -Backup-Label Backup_Label_Name-newsid New_sid-Host Target_Host-Label Clone_Label-commentcomment_Text-profileprofile_Name-clonepec full_path_to_clonespefile

     Oracle lässt Sie nicht zwei Datenbanken mit derselben SID gleichzeitig auf dem gleichen Host laufen. Aus diesem Grund müssen Sie für jeden Klon eine neue SID angeben. Sie können jedoch eine Datenbank auf einem anderen Host mit derselben SID haben.

Verwandte Informationen

Profile werden erstellt

Klonen von Datenbanken aus Backups

Erstellen von Klonspezifikationen

Der Befehl Smo Clone create

Anzeigen einer Liste von Klonen

Sie können eine Liste von Klonen anzeigen, die mit einem bestimmten Profil verknüpft sind.

Die Liste enthält die folgenden Informationen über die Klone in einem Profil:

- Die ID für den Klon
- Der Status des Klonvorgangs
- Oracle SID für den Klon
- Host, auf dem sich der Klon befindet
- Etikett für den Klon

Wenn Sie die Option -verbose angeben, werden in der Ausgabe auch die Kommentare für den Klon angezeigt.

1. Um eine Liste aller Klone für ein Profil anzuzeigen, geben Sie den folgenden Befehl ein: Smo Clone list -profile Profile_Name [-quiet / -verbose]

Verwandte Informationen

Der Befehl smo Clone list

Anzeigen detaillierter Kloninformationen

Mit dem Befehl Clone show können Sie ausführliche Informationen über einen bestimmten Klon anzeigen.

Mit dem Befehl Clone show werden die folgenden Informationen angezeigt:

- Systemidentifikation und Klon-ID klonen
- Status des Klonvorgangs
- Start- und Enddatum bzw. -Uhrzeit des Klons
- Klonbezeichnung
- Klonkommentar
- Backup-Label und -ID
- Quelldatenbank
- Start- und Endzeit des Backups
- Datenbankname, Tabellen und Datendateien
- Host-Name und Dateisysteme mit Datendateien
- Storage-System-Volumes und Snapshot-Kopien, die den Klon sichern
- Gibt an, ob der Klon mithilfe des Backups auf dem primären oder sekundären Storage erstellt wurde

  a. Geben Sie den folgenden Befehl ein: `smo clone show -profile profile_name [-label label | -id guid]`

Verwandte Informationen

Der Befehl smo Clone show

Klone werden gelöscht

Sie können die Klone löschen, wenn die Größe der Snapshot-Kopie zwischen 10 % und 20 % des Backups reicht. Dies garantiert außerdem, dass der Klon die aktuellsten Daten enthält.

Die Bezeichnung ist die eindeutige Kennung für jeden Klon in einem Profil. Sie können den Klon mit dem Klonnamen oder der ID, jedoch nicht mit der System-ID (SID) löschen.

Die Klon-SID und die Klonbezeichnung sind nicht identisch.

Wenn Sie einen Klon löschen, muss die Datenbank ausgeführt werden. Andernfalls werden viele Dateien und Verzeichnisse für den vorhandenen Klon nicht gelöscht. Dies führt zu mehr Arbeit, bevor ein weiterer Klon erstellt werden kann.

Die für bestimmte Oracle-Parameter im Klon angegebenen Verzeichnisse werden beim Löschen des Klons zerstört und sollten nur Daten für die geklonte Datenbank enthalten: Archivprotokoll-Ziele, Hintergrund-, Core- und BenutzerabDump-Ziele. Die Audit-Dateien werden nicht gelöscht.

Sie können einen Klon nicht löschen, wenn der Klon in anderen Vorgängen verwendet wird.

Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Klonlöschen sammeln.

1. Geben Sie folgenden Befehl ein: smo Clone delete -profile profile_Name [-Label guid] [-syspasswordsyspassword] [Login-usernamedb_username-password] db_password-portdb_Port] [-asminstance-asmusernameasm_username-asmpasswordasm_password][-Force][-dump][-quiet]

Beispiel

```
smo clone delete -profile targetdb1_prof1 -label sales0908_clone1
```

Verwandte Informationen

Der Befehl smo Clone delete

Durch das Aufteilen eines Klons

Mit SnapManager können Sie einen vorhandenen Klon aufteilen und managen, der mit der FlexClone Technologie erstellt wurde. In der FlexClone Technologie nutzen der Klon und die ursprüngliche Datenbank dieselben physischen Datenblöcke.

Bevor Sie den Split-Vorgang des Klons durchführen, können Sie wissen, dass die geschätzte Größe des zu teilenden Klons und der erforderliche Speicherplatz im Aggregat verfügbar sind.

Ein neues Profil wird von SnapManager generiert, wenn der Klonvorgang erfolgreich abgeschlossen ist. Wenn SnapManager das neue Profil nicht erstellt, können Sie manuell ein neues Profil erstellen. Mit dem neuen Profil können Datenbank-Backups erstellt, Daten wiederhergestellt und Klone erstellt werden. Wenn der Klonteilvorgang erfolgreich ist, unabhängig davon, ob das neue Profil erstellt wird oder nicht, werden die klonbezogenen Metadaten aus der Repository-Datenbank entfernt.

Sie können die folgenden Aufgaben für das Aufteilen von Klonen ausführen:

- Sehen Sie sich die Schätzung für die Teilung von Klonen an.
- Teilen Sie einen Klon auf einem primären Storage auf.
- Teilen Sie einen Klon auf einem sekundären Storage auf.
- Zeigen Sie den Status des Vorgangs „Clone Split“ an.
- Beenden Sie den Klon-Split-Vorgang.
- Zerstören Sie das Profil zusammen mit dem zugrunde liegenden Storage.
- Löschen Sie das Profil, das für einen geteilten Klon erstellt wurde.

Wenn Sie einen Klon vom übergeordneten Volume teilen, werden die dem geklonten Volume zugeordneten Snapshot Kopien gelöscht. Die für die geklonte Datenbank erstellten Backups vor dem Klonteilungsprozess können nicht verwendet werden, da die Snapshot-Kopien dieser Backups gelöscht werden und die Backups als veraltete Einträge im Repository verbleiben.

Anzeigen einer Schätzung für die Teilung von Klonen

Mit der Schätzung für die Aufteilung der Klone können Sie den insgesamt verfügbaren freien Speicherplatz auf dem Aggregat, die Menge an freigegebenem Speicherplatz

zwischen dem Klon und der ursprünglichen Datenbank und den ausschließlich vom Klon verwendeten Speicherplatz ermitteln. Darüber hinaus können Sie Datum und Uhrzeit der Erstellung des zugrunde liegenden Klons sowie das Alter des Klons anzeigen. Anhand dieser Schätzung entscheiden Sie, ob ein Klon geteilt wird oder nicht.

Um die Schätzung für die Teilung von Klonen anzuzeigen, müssen Sie den Profilnamen des ursprünglichen Klons sowie die Beschriftung oder die GUID des Klonvorgangs eingeben. Wenn sich der Klon in einem anderen Host befindet, können Sie den Host-Namen angeben.

1. Geben Sie den folgenden Befehl ein, um die Schätzung für die Teilung von Klonen anzuzeigen: `smo clone split-estimate -profileprofile [-hosthostname] [-labelclone-label | -idclone-id][-quiet | -verbose]`

Im folgenden Beispiel wird der Befehl für Schätzung für geteilten Storage für Klone angezeigt:

```
smo clone split-estimate

-profile p1 -label clone_test_label
```

Durch Aufteilen eines Klons auf primären oder sekundären Storage

Sie können den Klon mit dem Befehl „Clone Split“ teilen. Nach Abschluss der Klonabteilung werden die Klonmetadaten aus der Repository-Datenbank entfernt und das mit dem Klon verbundene Backup kann gelöscht oder freigegeben werden.

Das neue Profil, das nach dem erfolgreichen Split-Vorgang erstellt wurde, wird zum Verwalten des Split-Klons verwendet. Das neue Profil wird wie jedes andere bestehende Profil in SnapManager sein. Mit diesem Profil können Backup-, Wiederherstellungs- und Klonvorgänge durchgeführt werden.

Außerdem können Sie die E-Mail-Benachrichtigung für das neue Profil konfigurieren. Dadurch kann der Datenbankadministrator über den Status des Datenbankvorgangs benachrichtigt werden, der mit dem Profil durchgeführt wurde.

SnapManager unterstützt die Abtrennung, wenn sie nur auf einem FlexClone durchgeführt wird.

Wenn der Split-Vorgang fehlschlägt, wird eine entsprechende Fehlermeldung mit dem Grund für einen Fehler angezeigt. Der Status mehrerer Vorgänge wird auch im Betriebsprotokoll angezeigt. Beispiel:

```
--[ INFO] The following operations were completed:
Clone Split : Success
Profile Create : Failed
Clone Detach : Success
```

Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Klon-Split-Vorgang sammeln.

Nachdem Sie den Befehl „Clone Split“ eingegeben haben, sollten Sie den SnapManager Server erst beenden, wenn der Vorgang zur Teilung von Klonen gestartet wurde.

SnapManager generiert das Profil, auch wenn Sie keinen Wert für das Oracle Konto angeben (osccount und osgroup).

1. Geben Sie den folgenden Befehl ein: smo Clone Split -profileclone-profile-hostname [-labelclone-label-Label - -idclone-id]-split-labelsplit-Operation-Label-commentNew-profilew-profile-profile [-protosdneclmnum] { [-countname-admgmnecn] { [-promedmedmgmnesm_adym] [-bussnecmnym_adym_adym} }] [-budnmnmgmnmgmgmgmnecn_adym] [-adym_adym_adym_datmnmnmnmnmnmnmnmnmnym] [-datamin_promgmnmnym_adym_adym_adym] [-datacefym_adym_adym_adym_adym_adym_adym_adymn

Anzeigen des Status des Klonteilprozesses

Sie können den Fortschritt des geteilten Prozesses anzeigen, den Sie begonnen haben.

1. Um den Status des Split-Prozesses für Klone anzuzeigen, geben Sie den folgenden Befehl ein: `smo clone split-status -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-status -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Anzeigen des Ergebnisses des Klon-Split-Prozesses

Sie können das Ergebnis des von Ihnen gestarteten Klonteilprozesses anzeigen.

1. Geben Sie den folgenden Befehl ein, um das Ergebnis des Split-Prozesses für Klone anzuzeigen: `smo clone split-result -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-result -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Beenden des Klonteilprozesses

Sie können den laufenden Klon-Split-Prozess beenden.

Nachdem Sie den Split-Prozess beendet haben, können Sie ihn nicht mehr fortsetzen.

1. Geben Sie den folgenden Befehl ein, um den Klon-Split-Vorgang zu beenden: `smo clone split-stop -profileprofile [-hosthostname] [-labelsplit-label | -idsplit-id] [-quiet | -verbose]`

```
smo clone split-stop -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Löschen eines Profils

Sie können ein Profil löschen, solange es keine erfolgreichen Backups enthält, die derzeit in anderen Vorgängen verwendet werden. Sie können Profile löschen, die freigegebene oder gelöschte Backups enthalten.

1. Geben Sie den folgenden Befehl ein: `smo profile delete -profileprofile [-quiet | -verbose]`

   Sie können ein neues Profil löschen, das für die Klonteilung erstellt wurde. Beim Löschen wird die Warnmeldung „Wenn Sie das Profil löschen, können Sie das Profil nicht zerstören. Später wird in der SnapManager-Befehlszeilenschnittstelle angezeigt.

```
smo profile delete -profile AUTO-REVEN
```

Zerstören eines Profils

SnapManager ermöglicht Ihnen die Zerstörung des Profils, das mit dem Split-Klon (Datenbank) verbunden ist, sowie des zugrunde liegenden Storage. Vergewissern Sie sich vor der Zerstörung des Profils, dass Sie die zugehörigen Backups und Klone entfernen.

1. Um ein Profil zu zerstören, das mit dem Split Clone erstellt wurde, sowie die Split Clone Datenbank, geben Sie den folgenden Befehl ein: `smo profile destroy -profileprofile [-hosthostname] [-quiet | -verbose]`

```
smo profile destroy -profile AUTO-REVEN
```

Löschen eines Arbeitszyklus für die Teilung von Klonen aus einer Repository-Datenbank

Sie können einen Eintrag für den Klon-Arbeitszyklus aus einer Repository-Datenbank löschen.

1. Um einen Eintrag für den Klon-Splitvorgang aus einer Repository-Datenbank zu löschen, geben Sie den folgenden Befehl ein:Smo Clone Split-delete -profilprofile [-hosthostname] [-labelsplit-Label [-idsplit-id] [-quiet

```
smo clone split-delete -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

Einführung in Datensicherung in SnapManager

SnapManager unterstützt Datensicherung zum Schutz der Backups auf sekundären oder tertiären Storage-Systemen. Sie müssen SnapMirror und SnapVault Beziehungen zwischen den Quell- und Ziel-Volumes einrichten.

Wenn Sie Data ONTAP 7-Mode verwenden, bietet SnapManager durch die Integration mit Protection Manager (OnCommand Unified Manager) eine richtlinienbasierte Datensicherung. Dies automatisiert die Replizierung von SnapManager Backups auf einem primären Storage-System auf ein sekundäres Storage-System oder gar auf ein tertiäres Storage-System mithilfe von SnapVault oder SnapMirror Richtlinien, die vom Storage- oder Backup-Administrator in Protection Manager erstellt wurden. Die Aufbewahrung auf dem primären Storage wird von SnapManager auf Grundlage der während der Profilerstellung definierten Aufbewahrung und der während der Backup-Erstellung gekennzeichneten Aufbewahrungsklasse gesteuert. Die Aufbewahrung des sekundären Storage Backups wird durch die im Protection Manager definierte Richtlinie gesteuert.

Bei Verwendung von Clustered Data ONTAP bietet SnapManager 3.4 die Richtlinien *SnapManager_cDOT_Mirror* und *SnapManager_cDOT_Vault* für die Datensicherung. Beim Erstellen eines Profils können Sie diese Richtlinien abhängig von der SnapMirror oder SnapVault Beziehung auswählen, die mithilfe der Clustered Data ONTAP CLI oder System Manager erstellt wurde. Wenn Sie ein Backup erstellen und das Profil auswählen, für das Sie den Schutz aktiviert haben, werden die Backups auf einem sekundären Speichersystem geschützt.

Bei Verwendung von SnapManager 3.3.1 mit Clustered Data ONTAP wurden die Backups mithilfe von Post-Skripten gesichert, die bei der Erstellung von Profilen ausgewählt wurden. Wenn Sie diese Profile verwenden möchten, müssen Sie nach dem Upgrade auf SnapManager 3.4 die folgenden Vorgänge ausführen:

- Sie müssen die Profile aktualisieren, um entweder die Richtlinie *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* auszuwählen und das zur Datensicherung verwendete Post-Skript zu löschen.
- Nachdem Sie das Profil aktualisiert haben, um die *SnapManager_cDOT_Vault*-Richtlinie zu verwenden, müssen Sie vorhandene Backup-Pläne löschen und neue Zeitpläne erstellen, um das SnapVault-Label für die Backups anzugeben.
- Falls die Profile in SnapManager 3.3.1 erstellt wurden, ohne die Post-Skripte auszuwählen, müssen Sie die Profile aktualisieren, um entweder die Richtlinie *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* auszuwählen, um die Datensicherung zu ermöglichen.

Wenn Sie im sekundären Storage-System Backups verwenden, die mit Post-Skripten von SnapManager 3.3.1 gespiegelt oder archiviert wurden, können Sie diese Backups nicht zur Wiederherstellung oder zum Klonen mit SnapManager 3.4 verwenden.

Bei Verwendung von Clustered Data ONTAP unterstützt SnapManager 3.4.2 mehrere Sicherungsbeziehungen (SnapMirror und SnapVault) auf Quell-Volumes. Es wird nur eine SnapMirror- und eine SnapVault-Beziehung pro Volume unterstützt. Sie müssen separate Profile erstellen, die jeweils über die Richtlinie SnapManager_cDOT_Mirror und SnapManager_cDOT_Vault ausgewählt sind.

SnapDrive für Unix 5.3.2 und höher ist zur Verwendung mehrerer Sicherungsrichtlinien erforderlich.

Was sind Sicherungsrichtlinien

Sicherungsrichtlinien sind Regeln, die die Sicherheit von Datenbank-Backups regeln. Sie können die Schutzrichtlinien während der Erstellung des Profils auswählen.

Eine Schutzrichtlinie definiert die folgenden Parameter:

- Wann Kopien auf den sekundären Storage übertragen werden sollten
- Die maximale Datenmenge, die zu geplanten Zeiten übertragen werden soll
- Wie lange die Kopien der einzelnen Backup-Standorte aufbewahrt werden sollen

- Warnmeldungen und Fehlerschwellwerte für Verzögerungszeiten

Wenn Schutz aktiviert ist, erstellt SnapManager einen Datensatz für die Datenbank. Ein Datenset besteht aus einer Sammlung von Storage Sets und Konfigurationsinformationen, die ihren Daten zugeordnet sind. Zu den mit einem Datensatz verknüpften Speichersätzen zählen ein primärer Speichersatz für den Export von Daten auf Clients sowie der Satz an Replikaten und Archiven, die sich auf anderen Speichergruppen befinden. Datensätze stellen exportierbare Anwenderdaten dar. Wenn der Administrator den Schutz für eine Datenbank deaktiviert, löscht SnapManager den Datensatz.

Welche Schutzzustände sind

SnapManager zeigt den Status jedes Backups an. Administratoren müssen über die verschiedenen Zustände Bescheid wissen und den Status ihrer Backups überwachen.

Ein Datenbankbackup kann die folgenden Schutzzustände haben:

Status	Definition	Erklärung
Geschützt	Der Schutz wurde angefordert und wurde aktiviert.	Protection ist für das Backup in SnapManager aktiviert, und der Protection Manager hat das Backup erfolgreich auf andere physische Laufwerke kopiert (auch als sekundärer Storage bezeichnet). Wenn der Protection Manager ein Backup aus dem sekundären Storage aufgrund einer Aufbewahrungsrichtlinie entfernt, kann das Backup zu einem nicht geschützten Status zurückkehren.
Nicht geschützt	Schutz wurde angefordert, aber nicht abgeschlossen.	Der Schutz ist für das Backup aktiviert, aber das Backup wird nicht auf andere physische Laufwerke kopiert. Das Backup ist noch nicht geschützt oder der Schutz ist ausgefallen oder es war früher geschützt, ist aber nicht mehr geschützt. Wenn Sie ein Backup erstellen, wird der anfängliche Sicherungsstatus des Backups entweder nicht angefordert oder nicht geschützt. Wenn das Backup nicht geschützt ist, wird es bei der Übertragung auf den sekundären Storage geschützt.

Status	Definition	Erklärung
Nicht angefordert	Schutz wurde nicht angefordert.	Der Schutz für das Backup ist nicht aktiviert. Auf denselben physischen Festplatten (auch als lokales Backup bezeichnet) befindet sich eine logische Kopie der Daten. Wenn bei der Erstellung des Backups kein Schutz angefordert wird, wird der Schutz auf dem Backup immer als nicht angefordert angezeigt.

Was sind Ressourcen-Pools

Ein Ressourcen-Pool ist eine Sammlung von ungenutztem physischen Storage (z. B. Storage-Systeme oder Aggregate), aus dem neue Volumes oder LUNs bereitgestellt werden können, um Daten zu enthalten. Wenn Sie einem Ressourcen-Pool ein Storage-System zuweisen, sind alle Aggregate dieses Storage-Systems für die Bereitstellung verfügbar.

Storage-Administratoren weisen den Backup- und Spiegelungskopien über die Konsole des Protection Manager einen Ressourcen-Pool zu. Die Provisionierungsapplikation kann dann automatisch Volumes aus den physischen Ressourcen im Ressourcen-Pool bereitstellen, um Backups und Spiegelungskopien zu enthalten.

Für geschützte Profile zeigt SnapManager Informationen zu einem Profil an und gibt an, ob diesem Profil ein Speicherpool zugewiesen wurde. Ist dies nicht der Fall, wird das Profil als „nicht-konform“ bezeichnet. Nachdem dem Datensatz des entsprechenden Profils ein Speicherpool zugewiesen wurde, gilt das Profil als „konform“.

Allgemeines zu unterschiedlichen Sicherungsrichtlinien

Sie können verschiedene Richtlinien zum Schutz der Backups auf den sekundären oder tertiären Speichersystemen auswählen.

Wenn Sie Data ONTAP 7-Mode verwenden und SnapManager mit Protection Manager integriert ist, müssen Sie beim Erstellen des Profils eine der folgenden Sicherungsrichtlinien auswählen. Die Protection Manager Management Console bietet Vorlagen für die Konfiguration von Sicherungsrichtlinien für die Datensätze. Obwohl die Richtlinien für Disaster Recovery-Schutz in der Benutzeroberfläche von SnapManager aufgeführt sind, werden diese Richtlinien nicht unterstützt.

Richtlinie	Beschreibung
Backup	Ein Datensatz wird lokal und über SnapVault oder SnapMirror vom primären auf den sekundären Storage gesichert.

Richtlinie	Beschreibung
Zurück, dann Spiegel	Ein Datensatz wird mithilfe von SnapVault oder SnapMirror vom primären auf den sekundären Storage gesichert und dann zu einem SnapMirror Partner gespiegelt.
Nur lokale Snapshot-Kopien	Ein Datensatz verwendet nur lokale Snapshot-Kopien im Primär-Storage.
Spiegelung	Ein Datensatz wird mithilfe von SnapMirror vom primären zu einem sekundären Storage gespiegelt.
Spiegelung und Backup	Ein Datensatz wird mithilfe von SnapMirror vom primären zum sekundären Storage gespiegelt und anschließend mithilfe von SnapVault oder SnapMirror auf dem sekundären Storage gesichert.
Spiegelung und Spiegelung	Ein Datensatz wird von dem primären auf den sekundären Storage von zwei SnapMirror Partnern gespiegelt.
Spiegel, dann Backup	Ein Datensatz wird mithilfe von SnapMirror vom primären zum sekundären Storage gespiegelt und anschließend mithilfe von SnapVault oder SnapMirror auf tertiären Storage-Systemen gesichert.
Spiegeln, dann spiegeln	Ein Datensatz wird mithilfe von SnapMirror vom primären zum sekundären Storage gespiegelt und anschließend zu einem weiteren SnapMirror Partner gespiegelt.
Kein Schutz	Ein Datensatz verfügt über keine Snapshot Kopien, Backups oder Sicherungskopien beliebiger Spiegelungskopien.
Nur Remote Backup	Die Daten in einem Storage-System werden mithilfe von SnapVault oder SnapMirror Remote auf einem sekundären Storage gesichert. Die lizenzierte Applikation führt kein lokales Backup auf dem primären Storage durch. Diese Schutzrichtlinie kann auf Systeme anderer Hersteller angewendet werden, auf denen Open Systems SnapVault installiert ist.

Wenn Sie Clustered Data ONTAP verwenden, müssen Sie während der Erstellung des Profils eine der folgenden Schutzrichtlinien auswählen.

Richtlinie	Beschreibung

SnapManager_cDOT_Mirror	Spiegelung des Backups
SnapManager_cDOT_Vault	Vaults the Backup.

Konfiguration und Aktivierung richtlinienbasierter Datensicherung

Sie müssen SnapDrive und den DataFabric Manager-Server konfigurieren, um die Datensicherung im Profil zu ermöglichen, um Backups auf sekundären Storage-Systemen zu sichern. Sie können die Schutzrichtlinien in der Protection Manager-Konsole auswählen, um anzugeben, wie Datenbank-Backups geschützt werden sollen.

Sie müssen sicherstellen, dass OnCommand Unified Manager auf einem separaten Server installiert ist, um die Datensicherung zu ermöglichen.

Konfiguration des DataFabric Manager-Servers und des SnapDrive, wenn die RBAC aktiviert ist

Wenn die rollenbasierte Zugriffssteuerung aktiviert ist, müssen Sie den DataFabric Manager Server so konfigurieren, dass die RBAC-Funktionen enthalten sind. Sie müssen auch den im DataFabric Manager Server erstellten SnapDrive-Benutzer und den Root-Benutzer des Storage-Systems in SnapDrive registrieren.

1. Konfigurieren Sie den DataFabric Manager Server.
   a. Um den DataFabric Manager-Server zu aktualisieren, um die Änderungen, die direkt auf dem Storage-System durch die Ziel-Datenbank vorgenommen wurden, zu aktualisieren, geben Sie den folgenden Befehl ein:dfm Host discover Storage_System
   b. Erstellen Sie einen neuen Benutzer im DataFabric Manager-Server, und legen Sie das Passwort fest.
   c. Geben Sie zum Hinzufügen des Betriebssystembenutzers zur DataFabric Manager Server-Administratorliste den folgenden Befehl ein:dfm user add sd-admin
   d. Geben Sie zum Erstellen einer neuen Rolle im DataFabric Manager-Server den folgenden Befehl ein: dfm Role create sd-admin-role
   e. Um die Funktion DFM.Core.AccessCheck Global zur Rolle hinzuzufügen, geben Sie den folgenden Befehl ein:dfm-Rolle hinzufügen sd-admin-role DFM.Core.AccessCheck Global
   f. Geben Sie den folgenden Befehl ein, um dem Benutzer des Betriebssystems eine sd-Admin-Rolle hinzuzufügen:dfm-Benutzerrolle Set sd-adminsd-admin-role
   g. Geben Sie den folgenden Befehl ein, um eine weitere Rolle im DataFabric Manager Server für den SnapDrive-Root-Benutzer zu erstellen: dfm Role create sd-protect
   h. Um der Rolle, die für den SnapDrive-Root-Benutzer oder den Administrator erstellt wurde, RBAC-Funktionen hinzuzufügen, geben Sie die folgenden Befehle ein:dfm-Rolle hinzufügen sd-Protect SD.Config.Globaldfm lesen Rolle hinzufügen sd-protect SD.Config hinzufügen Globaldfm Rolle hinzufügen sd-Protect SD.Config.Globaldfm-Rolle löschen SD-Schutz hinzufügen SD.Database.Write Globaldfm-Rolle hinzufügen
   i. Um den oracle-Benutzer der Zieldatenbank zur Liste der Administratoren im DataFabric Manager Server hinzuzufügen und die sd-Protect-Rolle zu zuweisen, geben Sie den folgenden Befehl ein:dfm user add -r sd-protecttardb_host1\oracle
   j. Geben Sie zum Hinzufügen des von der Zieldatenbank verwendeten Speichersystems im DataFabric

Manager-Server den folgenden Befehl ein:dfm Host set Storage_System hostLogin=oracle hostPassword=password

k. Geben Sie zum Erstellen einer neuen Rolle in dem Storage-System, das von der Zieldatenbank im DataFabric Manager-Server verwendet wird, den folgenden Befehl ein:dfm Host Role create -h Storage_System-c „API-**,Login-**“ Storage-rbac-Role

l. Geben Sie zum Erstellen einer neuen Gruppe im Speichersystem und Zuweisen der neuen Rolle, die im DataFabric Manager Server erstellt wurde, den folgenden Befehl ein:dfm Host usergroup create -h Storage_System-r Storage-rbac-rolestorage-rbac-Group

m. Um einen neuen Benutzer im Storage-System zu erstellen und die neue Rolle und die im DataFabric Manager Server erstellte Gruppe zuzuweisen, geben Sie den folgenden Befehl ein:dfm Host user create -h Storage_System-r Storage-rbac-Role -p password -g Storage-rbac-grouptardb_host1

2. Konfigurieren Sie SnapDrive.

a. Geben Sie den folgenden Befehl ein, um die Anmeldedaten des sd-Admin-Benutzers mit SnapDrive zu registrieren: snapdrive config set -dfm sd-admindfm_Host

b. Um den Root-Benutzer oder den Administrator des Speichersystems mit SnapDrive zu registrieren, geben Sie den folgenden Befehl ein:snapdrive config set tardb_Host 1stenorage_System

SnapDrive konfigurieren, wenn die RBAC nicht aktiviert ist

Sie müssen den Root-Benutzer oder den Administrator des DataFabric Manager Servers und den Root-Benutzer des Storage-Systems mit SnapDrive registrieren, um die Datensicherung zu ermöglichen.

1. Geben Sie den folgenden Befehl ein, um den DataFabric Manager-Server zu aktualisieren, um die Änderungen direkt auf dem Storage-System durch die Zieldatenbank zu aktualisieren:

   dfm Host discover Storage_System

2. Geben Sie den folgenden Befehl ein, um den Root-Benutzer oder den Administrator des DataFabric Manager Servers mit SnapDrive zu registrieren:

   SnapDrive config set -dfm Administrstratordfm_Host

3. Geben Sie den folgenden Befehl ein, um den Root-Benutzer oder den Administrator des Speichersystems mit SnapDrive zu registrieren:

   SnapDrive-Konfiguration legt Root Storage_System fest

Allgemeines zum Aktivieren oder Deaktivieren von Datenschutz in Profil

Sie können den Datenschutz beim Erstellen oder Aktualisieren eines Datenbankprofils aktivieren oder deaktivieren.

Um ein geschütztes Backup einer Datenbank auf den sekundären Speicherressourcen zu erstellen, führen Datenbank- und Storage-Administratoren folgende Aktionen durch.

Ihr Ziel ist	Dann…
Erstellen oder bearbeiten Sie ein Profil	So erstellen oder bearbeiten Sie ein Profil: • Backup-Sicherung für den sekundären Storage • Wenn Sie Data ONTAP 7-Mode verwenden und Protection Manager installiert haben, können Sie die Richtlinien auswählen, die vom Storage- oder Backup-Administrator in Protection Manager erstellt wurden. Wenn Sie Data ONTAP in 7-Mode verwenden und der Schutz aktiviert ist, erstellt SnapManager einen Datensatz für die Datenbank. Ein Datenset besteht aus einer Sammlung von Storage Sets und Konfigurationsinformationen, die ihren Daten zugeordnet sind. Zu den mit einem Datensatz verknüpften Speichersätzen zählen ein primärer Speichersatz für den Export von Daten auf Clients sowie der Satz an Replikaten und Archiven, die sich auf anderen Speichergruppen befinden. Datensätze stellen exportierbare Anwenderdaten dar. Wenn der Administrator den Schutz für eine Datenbank deaktiviert, löscht SnapManager den Datensatz. • Wenn Sie ONTAP verwenden, müssen Sie je nach erstellten SnapMirror oder SnapVault Beziehung entweder die Richtlinie *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* auswählen. Wenn Sie den Sicherungsschutz deaktivieren, wird eine Warnmeldung angezeigt, die angibt, dass der Datensatz gelöscht wird und die Wiederherstellung oder das Klonen von Backups für dieses Profil nicht möglich ist.
Profil anzeigen	Da der Storage-Administrator noch keine Storage-Ressourcen zur Implementierung der Sicherungsrichtlinie zugewiesen hat, wird das Profil sowohl in der grafischen SnapManager Benutzeroberfläche als auch in der Ausgabe des Profils als nicht konform angezeigt.
Weisen Sie Storage-Ressourcen in der Protection Manager Management Console zu	In der Protection Manager Management-Konsole zeigt der Storage-Administrator den ungeschützten Datensatz an und weist jedem Node des Datensatzes, der dem Profil zugeordnet ist, einen Ressourcen-Pool zu. Der Storage-Administrator stellt dann sicher, dass sekundäre Volumes bereitgestellt und Sicherungsbeziehungen initialisiert werden.

Ihr Ziel ist	Dann…
Sehen Sie sich das entsprechende Profil in SnapManager an	In SnapManager erkennt der Datenbankadministrator, dass sich das Profil sowohl in der grafischen Benutzeroberfläche als auch in der Befehlsausgabe des Profils in den Status „formant“ geändert hat, was bedeutet, dass Ressourcen zugewiesen wurden.
Erstellen Sie das Backup	• Wählen Sie das vollständige Backup aus. • Wählen Sie außerdem aus, ob das Backup geschützt werden soll, und wählen Sie die primäre Aufbewahrungsklasse (z. B. stündlich oder täglich) aus. • Wenn Sie Data ONTAP in 7-Mode verwenden und das Backup sofort auf sekundärem Storage schützen möchten, der den Protection Manager-Schutzzeitplan überwählt, geben Sie die Option -protectnow an. • Wenn Sie ONTAP verwenden und das Backup sofort auf dem sekundären Storage schützen möchten, geben Sie die Option „Schutz“ an. Die Option zum Schutz ist in Clustered Data ONTAP nicht verfügbar.
Backup anzeigen	Das neue Backup wird als geplant für den Schutz angezeigt, aber noch nicht geschützt (in der SnapManager-Schnittstelle und in der Ausgabe des Backup show-Befehls). Der Schutzstatus wird als „`not protected`“ angezeigt.
Zeigen Sie die Sicherungsliste an	Nachdem der Storage-Administrator überprüft hat, ob das Backup in den sekundären Speicher kopiert wurde, ändert SnapManager den Sicherungsstatus von „`not protected`“ in „`protected`“.

Wie SnapManager Backups auf dem lokalen Storage aufbewahrt

Mit SnapManager können Sie Backups erstellen, die Aufbewahrungsrichtlinien erfüllen, die angeben, wie viele erfolgreiche Backups auf lokalem Storage aufbewahrt werden sollen. Sie können die Anzahl erfolgreicher Backups angeben, die im Profil für eine bestimmte Datenbank aufbewahrt werden sollen.

Sie können Backups für folgende erstellen:

- 10 Tage tägliche Backups auf dem Primärspeicher
- 2 Monate monatliche Backups auf dem Primärspeicher

- 7 Tage tägliche Backups auf dem Sekundärspeicher
- 4 Wochen wöchentliche Backups auf dem Sekundärspeicher
- 6 Monate monatliche Backups auf dem Sekundärspeicher

Sie können für jedes Profil in SnapManager die Werte für die folgenden nicht begrenzten Aufbewahrungsklassen ändern:

- Stündlich
- Täglich
- Wöchentlich
- Monatlich

SnapManager legt fest, ob ein Backup aufbewahrt werden soll, indem sowohl die Anzahl der Aufbewahrung (z. B. 15 Backups) als auch die Aufbewahrungsdauer (z. B. 10 Tage tägliche Backups) berücksichtigt werden. Ein Backup läuft ab, wenn sein Alter die für seine Aufbewahrungsklasse festgelegte Aufbewahrungsdauer überschreitet oder die Anzahl der Backups die Aufbewahrungsdauer überschreitet. Beispiel: Wenn die Backup-Anzahl 15 beträgt (SnapManager hat 15 erfolgreiche Backups erstellt) und die Dauer für tägliche Backups von 10 Tagen festgelegt wird, laufen die fünf ältesten erfolgreichen geeigneten Backups ab.

Nach Ablauf eines Backups wird das abgelaufene Backup entweder von SnapManager entfernt oder gelöscht. SnapManager behält immer das letzte Backup bei.

SnapManager zählt nur die Anzahl erfolgreicher Backups für die Aufbewahrungszahl. Es werden folgende Punkte nicht berücksichtigt:

Backups, die nicht in der Aufbewahrungsanzahl enthalten sind	**Zusätzliche Angaben**
Fehlgeschlagene Backups	SnapManager behält die Informationen zu erfolgreichen und fehlgeschlagenen Backups bei. Obwohl fehlgeschlagene Backups nur einen minimalen Speicherplatz im Repository benötigen, können Sie diese auch löschen. Fehlgeschlagene Backups verbleiben im Repository, bis Sie sie löschen.
Backups, die für die Aufbewahrung vorgesehen sind, unbegrenzt oder für eine andere Aufbewahrungsklasse Backups	SnapManager löscht keine Backups, die für die Aufbewahrung vorgesehen sind. Darüber hinaus berücksichtigt SnapManager nur die Backups in derselben Aufbewahrungsklasse (beispielsweise berücksichtigt SnapManager nur die stündlichen Backups für die stündliche Aufbewahrungszahl).
Backups werden über lokalen Storage gemountet	Wenn Snapshot Kopien angehängt werden, sind sie auch geklont und gelten somit nicht als für die Aufbewahrung geeignet. SnapManager kann die Snapshot Kopien nicht löschen, wenn sie geklont sind.

Backups, die nicht in der Aufbewahrungsanzahl enthalten sind	Zusätzliche Angaben
Backups, die zum Erstellen eines Klons im lokalen Storage verwendet werden	SnapManager behält alle Backups, die zum Erstellen von Klonen verwendet werden, berücksichtigt diese jedoch nicht für die Anzahl der Backup-Aufbewahrung.
Backups, die geklont oder auf sekundärem Storage eingebunden sind und die Sicherungsrichtlinie für Spiegelung nutzen	Wenn SnapManager die Snapshot Kopien für das Backup der primären Storage-Ressource löscht und die Snapshot-Kopien gespiegelt werden, schlägt das nächste Backup auf dem sekundären Storage fehl.

Wenn Sie ein Backup der primären Speicherressourcen freigeben, werden die vom Backup verwendeten primären Ressourcen (Snapshot-Kopien) zerstört, die Backup-Metadaten sind aber weiterhin verfügbar. SnapManager berücksichtigt keine freigegebenen Backups in der Anzahl der Backup-Aufbewahrung.

SnapManager bietet für jede Aufbewahrungsklasse eine Standardanzahl und -Dauer. Beispielsweise behalten SnapManager für die Anzahl der stündlichen Aufbewahrungsklassen standardmäßig vier Backups pro Stunde bei. Sie können diese Standardwerte überschreiben und beim Erstellen oder Aktualisieren des Profils die Werte festlegen oder die Standardwerte für die Anzahl und Dauer der Aufbewahrung in der Datei smo.config ändern.

Backups auf dem Primärspeicher können durch das Backup auf dem Sekundärspeicher gesichert werden. Während SnapManager die Aufbewahrung und Planung von Backups auf dem primären Storage managt, managt der Protection Manager die Aufbewahrung und die Planung von Backups auf dem sekundären Storage.

Wenn lokale Backups aufgrund ihrer Aufbewahrungsrichtlinien ablaufen, werden sie je nach Sicherungsdatum gelöscht oder freigegeben.

- Sind sie geschützt, werden die lokalen Backups freigegeben. Ihre Storage-Ressourcen oder Snapshot-Kopien werden gelöscht, die Backups verbleiben jedoch im SnapManager-Repository und sind für die Wiederherstellung aus dem sekundären Storage verfügbar. Sie müssen keine Backups freigeben (z. B. mit dem Befehl Backup free). Backups werden freigegeben, bis der Backup nicht mehr im Sekundärspeicher vorhanden ist und dann das Backup gelöscht wird.
- Sind sie nicht geschützt, werden die lokalen Backups gelöscht.

Bei einem nur-archivlog Backup Vorgang archiviert SnapManager die Redo-Log-Dateien nicht, anders als beim Online-Datenbank-Backup-Prozess. Sie müssen ein Pre-Task-Skript hinzufügen, um die Redo-Log-Dateien zu archivieren, bevor Sie den nur-Archivprotokoll durchführen. Das Vortaskskript muss den Befehl Logfile ändern System Switch ausführen.

Das folgende Beispiel zeigt die Maßnahmen, die SnapManager für verschiedene Arten von Backups ergreift, basierend auf einer Aufbewahrungsrichtlinie für drei tägliche Backups (wobei die Anzahl auf Aufbewahrung 3 festgelegt ist):

Backup-Datum	Status	Maßnahmen zur Aufbewahrungsrichtlinie ergriffen	Erklärung

5/10	Erfolgreich	Bitte Halten	Es handelt sich um das aktuellste erfolgreiche Backup und wird daher beibehalten.
5/9	Erfolgreich, geklont	Überspringen	SnapManager berücksichtigt keine Backups, die zum Klonen in der Anzahl der Aufbewahrungsrichtlinien verwendet werden. Dieses Backup entfällt auf die Anzahl erfolgreicher Backups.
5/8	Erfolgreich, angehängt	Überspringen	SnapManager berücksichtigt keine gemounteten Backups in der Anzahl der Aufbewahrungsrichtlinien. Dieses Backup entfällt auf die Anzahl erfolgreicher Backups.
5/7	Fehlgeschlagen	Überspringen	Fehlgeschlagene Backups werden nicht gezählt.
5/5	Erfolgreich	Bitte Halten	SnapManager hält dieses zweite erfolgreiche tägliche Backup.
5/3	Erfolgreich	Bitte Halten	SnapManager hält dieses dritte erfolgreiche tägliche Backup.
5/2	Erfolgreich	Löschen	SnapManager zählt dieses erfolgreiche Backup, aber nachdem SnapManager drei erfolgreiche tägliche Backups erreicht hat, wird dieses Backup gelöscht.

Verwandte Informationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Überlegungen zur Durchführung der Datensicherung

Beachten Sie bei der Durchführung von Datensicherung bestimmte Überlegungen.

- Um Klon- oder Wiederherstellungsvorgänge von sekundären Systemen durchzuführen, müssen Sie das Ziel-Volume im Namespace mounten und ordnungsgemäß exportieren.
- Sie müssen den SnapDrive-Konfigurationsparameter „Check-Export-Permission-nfs-Clone“ deaktivieren, indem Sie den Wert auf „aus“ setzen.

  Die Dokumentation zu SnapDrive für UNIX auf der NetApp Support-Website enthält zusätzliche Informationen zum Parameter Check-Export-Permission-nfs-Clone.

- Sie müssen die SnapMirror Beziehung für die angeforderten sekundären Storage-Volumes im sekundären Storage-System konfigurieren.
- Sie müssen die SnapVault-Beziehung für die angeforderten sekundären Storage-qtrees im sekundären Storage-System für Data ONTAP 7-Mode konfigurieren.
- Sie müssen eine Richtlinie und Regeln für das benutzerdefinierte SnapMirror-Etikett definieren, wenn Sie SnapVault Post-Script für Clustered Data ONTAP verwenden.

  SnapVault Post-Script unterstützt geclusterte Data ONTAP Volumes und die SnapMirror Beziehungstypen DP und XDP. Die ONTAP-Dokumentation auf der NetApp Support-Website enthält Informationen zur Konfiguration von SnapMirror und SnapVault.

- In NAS-Umgebungen müssen Sie den primären und sekundären NAS-Datenpfad mithilfe des befehls SnapDrive config set-mgmtpathmanagement_pathmanagement_pathmanagement_pathdatapath_path konfigurieren.

  zum Beispiel SnapDrive config set -mgmtpath f3050-197-91 f3050-197-91 f3050-197-91 f3050-220-91, wobei `f3050-197-91` Ist der Managementpfad und `f3050-220-91` Ist der Datenpfad.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Lizenzen für Datensicherung in SnapManager erforderlich

Sie müssen sicherstellen, dass die für die Datensicherung erforderlichen Lizenzen auf den primären und sekundären Storage-Systemen installiert und aktiviert werden.

Primäre Speichersysteme erhalten die aktuellsten Transaktions-Updates für die Oracle-Datenbank, speichern die Daten und stellen lokalen Backup-Schutz der Datenbank sicher. Das primäre Storage-System verwaltet außerdem Datenbankdatendateien, Log-Dateien und Kontrolldateien. Sekundäre Speichersysteme fungieren als Remote-Speicher für die geschützten Backups.

Zur Datensicherung müssen auf den primären Storage-Systemen die folgenden Lizenzen installiert und aktiviert sein:

> Wenn Sie die Datensicherung auf den sekundären Storage-Systemen aktivieren möchten, müssen Sie diese Lizenzen auch auf den sekundären Storage-Systemen installieren und aktivieren.

- Data ONTAP 7-Mode (7.3.1 oder höher) oder Clustered Data ONTAP (8.2 oder höher)
- SnapVault (je nach Schutzrichtlinie)

- SnapRestore
- SnapMirror (abhängig von der Sicherungsrichtlinie)
- Für das Network File System (NFS) und Klonen ist FlexClone erforderlich.

  FlexClone ist außerdem nur erforderlich, wenn SnapDrive für die Verwendung von FlexClone in SAN-Umgebungen konfiguriert ist.

- Das entsprechende Protokoll, z. B. NFS, Internet Small Computer System Interface (iSCSI) oder Fibre Channel (FC)

SnapVault oder SnapMirror sollten sich auf den primären und sekundären Storage-Systemen basierend auf den verwendeten Sicherungsrichtlinien befinden. Für grundlegende Backup-Sicherungsrichtlinien ist nur SnapVault auf den zugehörigen Systemen installiert. Für Richtlinien mit Spiegelschutz muss SnapMirror auf den unterstützenden Systemen installiert werden. Für die Disaster Recovery-Richtlinien für Backup und Spiegelung ist SnapMirror auf den unterstützenden Systemen installiert.

Sicherung von Datenbank-Backups auf sekundärem oder tertiärem Storage

Die Backup-Kopien können mit SnapManager auf sekundären oder tertiären Storage-Systemen gesichert werden.

1. Geben Sie den folgenden Befehl ein: `smo backup create -profile profile_name {[-full {-online | -offline | -auto} [-retain {-hourly | -daily | -weekly | -monthly | -unlimited}] [-verify] | [-data [[-filesfiles [files]] | [-tablespaces-tablespaces [-tablespaces]] [-datalabellabel] {-online | -offline | -auto} [-retain {-hourly | [-daily | -weekly | -monthly | -unlimited]} [-verify] | [-archivelogs [-labellabel] [-commentcomment] [-snapvaultlabelSnapVault_label][-protect | -noprotect | -protectnow] [-backup-destpath1 [,[path2]]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all | -untilSCNuntilSCN | -until-date yyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}} -prune -destprune_dest1,[prune_dest2]] [-taskspectaskspec]} [-dump] [-force] [-quiet | -verbose]`

Ihr Ziel ist	Dann tun Sie das…
Erstellen Sie eine Sicherung einer Online- oder Offline-Datenbank, anstatt SnapManager zu verwalten, ob es online oder offline ist	Geben Sie die Option -offline oder -online an, um ein Backup der Offline-Datenbank oder der Online-Datenbank zu erstellen. Wenn Sie die Option -offline oder -online verwenden, können Sie die Option -Auto nicht verwenden.
Lassen Sie SnapManager das Sichern einer Datenbank verwalten, unabhängig davon, ob sie online oder offline ist	Geben Sie die Option -Auto an. Wenn Sie die Option -Auto verwenden, können Sie die Option -offline oder -online nicht verwenden.
Fügen Sie einen Kommentar zum Backup	Geben Sie die Option -comment an, gefolgt von der Beschreibungszeichenfolge.

Ihr Ziel ist	Dann tun Sie das…
Erzwingen Sie die Datenbank in den Zustand, in dem Sie angegeben haben, sie zu sichern, unabhängig vom Zustand, in dem sie sich derzeit befindet	Geben Sie die Option -Force an.
Überprüfen Sie die Sicherung zum Zeitpunkt der Erstellung	Geben Sie die Option -verify an.
Erstellen Sie ein Backup auf dem sekundären Speicher	Geben Sie die Option -protect an. • Wenn Sie ONTAP verwenden und das Backup sofort auf dem sekundären Storage sichern möchten, geben Sie die Option -protect an. Die Option -protectnow ist in Clustered Data ONTAP nicht anwendbar. • Wenn Sie Data ONTAP in 7-Mode verwenden und das Backup sofort auf sekundärem Storage schützen möchten, der den Protection Manager-Schutzzeitplan überwählt, geben Sie die Option -protectnow an. • Um das Backup auf den sekundären Speicher zu verhindern, geben Sie die Option -noprotect an. Wenn Sie ONTAP verwenden und beim Erstellen des Profils die Schutzrichtlinie *SnapManager_cDOT_Vault* ausgewählt haben, müssen Sie die Option -snapvaultltlabel angeben. Sie müssen das SnapMirror-Label bereitstellen, das Sie in den Regeln der SnapMirror-Richtlinie angegeben haben, und gleichzeitig die SnapVault-Beziehung als Wert einrichten.
Geben Sie die Werte der Aufbewahrungsklasse an	Geben Sie die Option -Retention an und geben Sie an, ob das Backup beibehalten werden soll, abhängig von einer der folgenden Aufbewahrungsklassen: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • -Unlimited Wenn Sie nicht die Aufbewahrungsklasse angeben, verwendet SnapManager standardmäßig -hourly.

Beispiele

Mit dem folgenden Befehl wird ein Datenbank-Backup geschützt:

```
smo backup create -profile PAYDB -protect -retain -daily -full auto -label
full_bkup_sales
```

Mit dem folgenden Befehl wird ein Datenbank-Backup sofort geschützt:

```
smo backup create -profile PAYDB -protectnow -retain -daily -full auto
-label full_bkup_sales
```

Wiederherstellen geschützter Backups aus dem sekundären Speicher

Sie können geschützte Backups aus dem sekundären Storage wiederherstellen. Sie können jedoch keine Backups aus dem Sekundärspeicher wiederherstellen, wenn das Backup auch auf dem Primärspeicher vorhanden ist.

Verwandte Informationen

Der Smo Backup Restore Befehl

Wiederherstellen von Backups von einem alternativen Speicherort

Erstellen von Wiederherstellungsspezifikationen

Wiederherstellung von geschützten Backups – Übersicht

Sie können die Wiederherstellungsmethode wählen, mit der die Backup-Daten vom sekundären Storage in den primären Storage wiederhergestellt werden sollen.

In der folgenden Tabelle werden die verschiedenen Szenarien und Methoden erläutert, die zum Wiederherstellen eines Backups aus dem sekundären Storage verwendet werden können:

Ziel wiederherstellen	Erklärung
Direkt auf den Primärspeicher	Liefert die Daten vom sekundären Storage-System direkt an den ursprünglichen Standort auf dem primären Storage-System über dasselbe Netzwerk zurück, das zur Sicherung der Daten verwendet wurde. SnapManager verwendet, wann immer dies möglich ist, die Methode Direct Storage. Diese Methode ist nicht möglich, wenn sich die Daten in einem Dateisystem im Storage Area Network (SAN) befinden und wenn eine der folgenden Bedingungen gelten: • Andere nicht aus Datenbanken stammende Dateien werden nicht im selben Dateisystem wiederhergestellt. • Es wurden Snapshot Kopien der Kontrolldateien und Datendateien in einem wiederherzustellenden Filesystem zu unterschiedlichen Zeiten erstellt. • Die Logical Unit Number (LUN) befindet sich in einer Volume-Gruppe, aber andere LUNs in derselben Volume-Gruppe werden nicht wiederhergestellt.
Direkt zum Host	Klonen der Daten auf dem sekundären Storage-System und Mounten der geklonten Daten auf dem Host Nachdem die Daten geklont und gemountet wurden, kopiert SnapManager sie am ursprünglichen Speicherort.

Ziel wiederherstellen	Erklärung
Indirekt zu Storage oder Host	Liefert die Daten aus dem sekundären Storage-System an einen neuen Standort auf dem Primärsystem über dasselbe Netzwerk zurück, mit dem die Daten gesichert und der neue Storage auf dem Host gemountet werden konnte. Nachdem die Daten zurückgegeben und gemountet wurden, kopiert SnapManager sie am ursprünglichen Speicherort. Die Rückgabemethode für indirekte Speicher kann eine lange Zeit in Anspruch nehmen. SnapManager kopiert Daten zunächst auf ein Scratch Volume auf dem primären Host, bevor SnapManager es zum Wiederherstellen und Wiederherstellen der Datenbank verwendet. Ob die Scratch-Daten automatisch gelöscht werden, hängt vom verwendeten Protokoll ab. • Bei SAN löscht SnapManager die zurückgegebenen Daten. • Bei Network-Attached Storage (NAS) löscht SnapManager den Inhalt der zurückgegebenen qtrees, löscht jedoch nicht die qtrees selbst. Um die qtrees zu löschen, sollten Administratoren das Scratch Volume mounten und die qtrees mit dem UNIX rmdir Befehl entfernen.

Wenn Sie Daten nicht direkt an den Storage zurückgeben können, kann SnapManager Daten entweder direkt an den Host oder indirekt an den Storage oder den Host zurückgeben. Die Methode hängt von der Richtlinie ab, in der festgelegt wird, ob das Unternehmen eine direkte Verbindung zum sekundären Storage zulässt oder dass Daten über das Storage-Netzwerk kopiert werden müssen. Sie können diese Richtlinie verwalten, indem Sie Konfigurationsinformationen in die Datei smo.config setzen.

Verwandte Informationen

SnapManager-Konfigurationsparameter

Wiederherstellung von Backups aus dem sekundären Storage

Sie können geschützte Backups von sekundärem Storage wiederherstellen und wählen, wie die Daten zurück auf den primären Storage kopiert werden sollen.

Sie können den Befehl zur Wiederherstellung der Sicherung mit der Option -from-secondary verwenden, um die Daten aus dem sekundären Storage wiederherzustellen. Wenn Sie die Option -from-secondary nicht angeben, stellt SnapManager die Daten aus den Snapshot Kopien im Primärspeicher wieder her.

Sie können die Option -von-sekundär nicht verwenden, wenn das Backup auf dem Primärspeicher vorhanden ist. Das primäre Backup muss freigegeben werden, bevor ein Backup aus dem Sekundärspeicher wiederhergestellt werden kann. Wenn Sie ein temporäres Volumen verwenden, müssen Sie das Volumen mithilfe der Option -temp-Volume angeben.

Sie müssen die Option -copy-id angeben, wenn Sie die Option -from-secondary angeben. Wenn auf dem

sekundären Speichersystem mehrere Backups vorhanden sind, wird mit der Option -copy-id angegeben, welche Backup-Kopie auf dem sekundären Speicher für den Wiederherstellungsvorgang verwendet werden soll.

Wenn Sie Data ONTAP in 7-Mode verwenden, müssen Sie einen gültigen Wert für die Option -copy-id angeben. Wenn Sie jedoch Clustered Data ONTAP verwenden, ist die Option -copy-id nicht erforderlich.

Beim Wiederherstellen von Daten aus dem Sekundärspeicher versucht SnapManager zunächst, Daten direkt aus dem sekundären Speichersystem auf dem primären Speichersystem (ohne Beteiligung des Hosts) wiederherzustellen. Wenn SnapManager diese Art der Wiederherstellung nicht durchführen kann (z. B. wenn die Dateien nicht Teil des Dateisystems sind), dann wird SnapManager zurück zu einer Host-seitigen Dateikopie zurückkehren. SnapManager verfügt über zwei Methoden zur Wiederherstellung einer Host-seitigen Dateikopie aus dem sekundären Storage. Die von SnapManager gewählte Methode wird in der smo.config-Datei konfiguriert.

- Wenn restore.secondaryAccessPolicy = direkt, klont SnapManager die Daten auf dem sekundären Storage, bindet die geklonten Daten vom sekundären Storage-System an den Host und kopiert sie anschließend Daten aus dem Klon in die aktive Umgebung.

  Dies ist die standardmäßige sekundäre Zugriffsrichtlinie.

- Wenn restore.secondaryAccessPolicy = indirekt, kopiert SnapManager die Daten zuerst auf ein temporäres Volume im Primärspeicher, bindet die Daten vom temporären Volume an den Host und kopiert dann Daten aus dem temporären Volume in die aktive Umgebung.

  Diese Richtlinie sollte nur verwendet werden, wenn der Host keinen direkten Zugriff auf das sekundäre Speichersystem hat. Wiederherstellungen mit der indirekten Methode dauern doppelt so lange wie die direkte Methode, da zwei Kopien der Daten erstellt werden.

  a. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Dann…
Stellen Sie eine vollständige Datenbank wieder her, wenn das ausgewählte Backup auf dem primären Speicher vorhanden ist	Geben Sie den folgenden Befehl ein: smo Backup Restore -profileprofile_Name-labellabel-complete -Recovery -alllogs[-copy-idid]
Stellen Sie eine vollständige Datenbank wieder her, wenn das ausgewählte Backup nicht im primären Speicher vorhanden ist	Geben Sie den folgenden Befehl ein: smo Backup Restore -profileprofile_Name-labellabel-complete -recover -alllogs-from-secondary [-temp-Volume <temp_Volume>] [-copy-idid]

Beispiel

Mit dem folgenden Befehl wird ein geschütztes Backup aus dem sekundären Speichersystem wiederhergestellt:

```
smo backup restore -profile PAYDB -label daily_monday -complete
-recover alllogs -from-secondary -copy-id 3042 -temp-volume
smo_scratch_restore_volume
Operation Id [8abc011215d385920115d38599470001] succeeded.
```

Klonen geschützter Backups

Sie können SnapManager verwenden, um eine Kopie eines geschützten Backups zu klonen.

Der Host (für den Klon ausgewählt) muss über dasselbe Storage-Protokoll (z. B. SAN oder NAS) Zugriff auf den sekundären Storage haben.

Sie können mit der Option -from-secondary angeben, dass Sie aus dem sekundären Storage klonen möchten.

Sie müssen die Option -copy-id angeben, wenn Sie die Option -from-secondary angeben. Wenn auf dem sekundären Speichersystem mehrere Backups vorhanden sind, wird mit der Option -copy-id angegeben, welche Backup-Kopie auf dem sekundären Speicher zum Klonen verwendet werden soll.

Wenn Sie Data ONTAP in 7-Mode verwenden, müssen Sie einen gültigen Wert für die Option -copy-id angeben. Wenn Sie jedoch Clustered Data ONTAP verwenden, ist die -copy-idOption nicht erforderlich.

Das Löschen der Klone geschützter Backups auf sekundären Storage-Systemen kann fehlschlagen. Dieses Problem tritt auf, wenn die Systemzeit des primären und sekundären Storage-Systems nicht synchronisiert wird.

1. Erstellen Sie einen Klon einer geschützten Backup-Kopie: smo Clone create -Backup-labelBackup_Name -newsidNew_sid-labelclone_Label-profilprofile_Name-clonespepfull_path_to_clonespepfile-from-secondary -copy-idid

Beispiel

```
smo clone create -label testdb_clone_clstest
-profile sys_db_finance -from-secondary -copy-id 3042
sys_db_finance_sept_08
```

SnapManager für Oracle verwendet Protection Manager, um ein Datenbank-Backup zu schützen

Wenn SnapManager für Oracle und Protection Manager auf einem UNIX-Host bzw. auf dem Server installiert sind, geben Sie dem SnapManager Datenbankadministrator (DBA) die Möglichkeit, richtlinienbasierte Oracle-Datenbank-Backups auf Sekundärspeicher zu konfigurieren und durchzuführen, Und zur Wiederherstellung, falls erforderlich, die gesicherten Daten aus dem sekundären- auf dem primären Storage.

Im folgenden Beispiel erstellt ein DBA, der SnapManager nutzt, ein Profil für ein lokales Backup im primären Storage und ein weiteres Profil für ein geschütztes Backup im Sekundärspeicher. Anschließend arbeitet dieser DBA mit seinem Netzwerk-Storage-Administrator, der die Protection Manager-Konsole verwendet, zusammen, um ein richtlinienbasiertes Backup dieser Datenbank vom primären zum sekundären Storage zu konfigurieren.

Details der Zieldatenbank

Dieses Beispiel eines integrierten Datenbankschutzes beschreibt den Schutz einer Gehaltsabrechnungsdatenbank. Im Beispiel werden die folgenden Daten verwendet.

Der Datenbankadministrator (DBA) von TechCo, einem Unternehmen mit 3000 Personen mit Hauptsitz in Atlanta, muss ein konsistentes Backup der Gehaltsabrechnungsdatenbank für die Produktion, PAYDB, erstellen. Zur Sicherungsstrategie für das Backup im primären und sekundären Storage müssen DBA und der Storage-Administrator gemeinsam die Oracle Datenbank sowohl lokal auf dem Primärspeicher als auch Remote auf dem Sekundärspeicher an einem Remote-Standort sichern.

- **Profilinformationen**

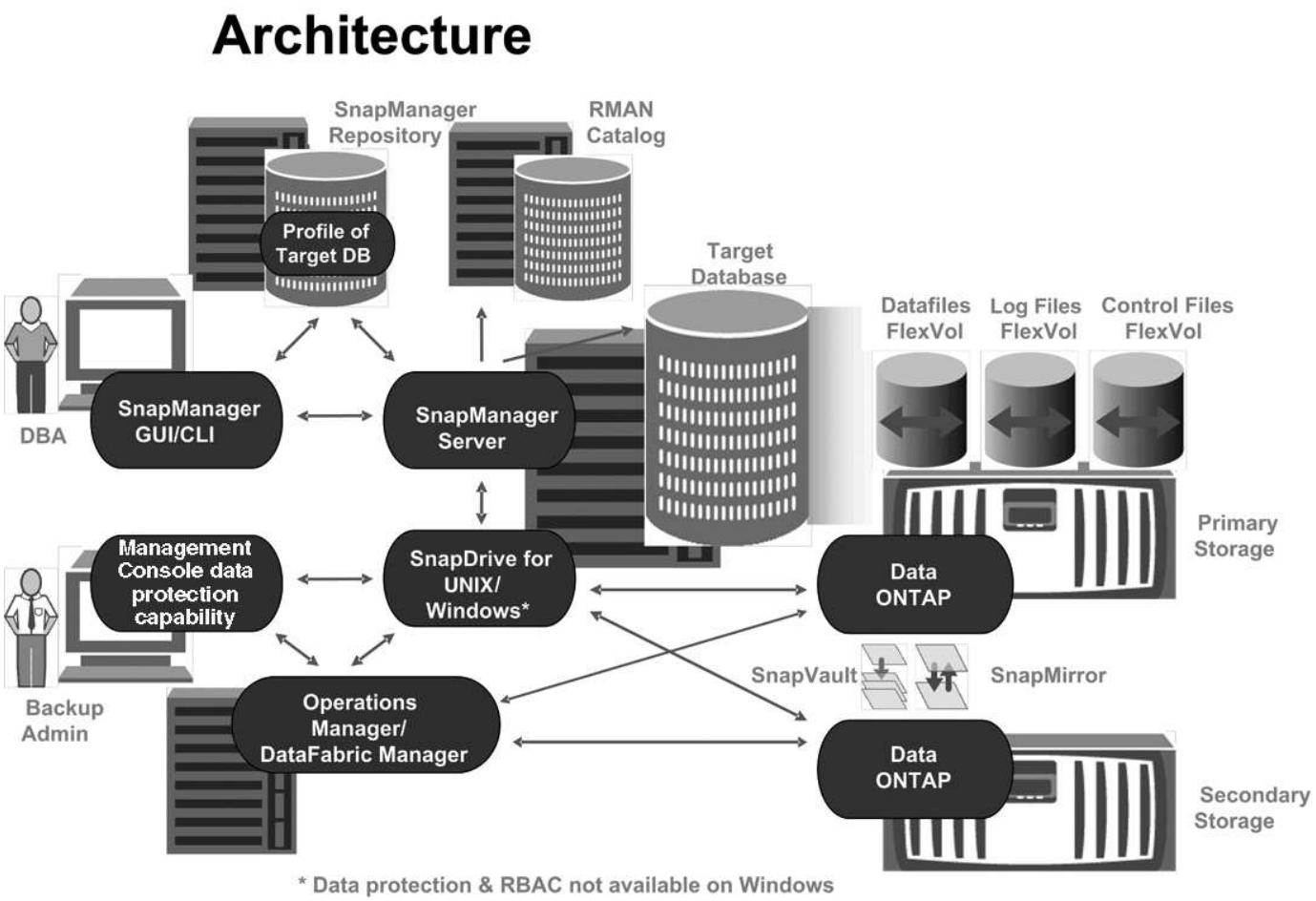
  Wenn Sie ein Profil in SnapManager erstellen, benötigen Sie die folgenden Daten:

  - Datenbankname: PAYDB
  - Host-Name: payroll.techco.com
  - Datenbank-ID: Payrolldb
  - Profilname: Gehaltsabrechnung_Prod
  - Verbindungsmodus: Datenbankauthentifizierung
  - Snapshot Benennungsschema: smo_Hostname_dbsid_smoprofile_scope_Mode_smid (übersetzt in „smo_payroll.xyz.com_payrolldb_payroll_prod_f_h_x")

Konfiguration und Topologie des primären und sekundären Storage

In diesem Beispiel betreibt die TechCo-Corporation ihre Gehaltsabrechnungsdatenbank auf einem Datenbankserver, der auch ein SnapManager für Oracle-Host ist und seine Gehaltsabrechnungsdaten und Konfigurationsdateien auf Primär-Storage-Systemen an der Unternehmenszentrale speichert. Die unternehmenseigene Anforderung besteht darin, die Datenbank mit täglichen und wöchentlichen Backups auf dem lokalen Storage sowie Backups auf den Storage-Systemen an einem rund 50 Kilometer entfernten sekundären Storage-Standort zu sichern.

Die folgende Abbildung zeigt die SnapManager für Oracle und die Datensicherungskomponenten der NetApp Management Console, die zur Unterstützung des lokalen und sekundären Backup-Schutzes erforderlich sind.



Für das Management der Gehaltsabrechnungsdatenbank und für Unterstützung des lokalen und sekundären Backup-Schutzes, wie in der vorherigen Grafik dargestellt, wird die folgende Implementierung verwendet.

- **SnapManager-Host**

  Der SnapManager Host, payroll.techco.com, befindet sich in der Unternehmenszentrale und wird auf einem UNIX Server ausgeführt, auf dem auch das Datenbankprogramm ausgeführt wird, das die Gehaltsabrechnungsdatenbank generiert und verwaltet.

  - **Verbindungen**

    Zur Unterstützung von lokalem Backup und sekundärem Backup-Schutz verfügt der SnapManager-Host über Netzwerkverbindungen mit den folgenden Komponenten:

    - SnapManager für Oracle Client
    - SnapManager-Repository für das Datenbankprogramm, SnapDrive für UNIX und SnapManager
    - Primärspeicher
    - Sekundäre Storage-Systeme
    - DataFabric Manager Server
  - **Installierte Produkte**

    Der SnapManager Host wird für dieses Beispiel mit den folgenden Produkten installiert:

    - SnapManager Server

        - SnapDrive für UNIX
        - Host Utilities
- **TechCo Primärspeichersysteme**

  Die Gehaltsabrechnungsdatenbank, einschließlich zugehöriger Datendateien, Log-Dateien und Kontrolldateien, befindet sich in den primären Storage-Systemen. Diese befinden sich am Hauptsitz des Unternehmens TechCo sowie am SnapManager Host und am Netzwerk, das primären Storage mit dem SnapManager Host verbindet. Die neuesten Transaktionen und Updates der Gehaltsabrechnung von Datenbanken werden auf die primären Storage-Systeme geschrieben. Snapshot-Kopien, die einen lokalen Backup-Schutz der Gehaltsabrechnungsdatenbank bieten, befinden sich auch auf dem primären Storage-System.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügen die primären Speichersysteme über Netzwerkverbindungen mit den folgenden Komponenten:

    - Auf dem SnapManager Host wird das Datenbankprogramm, SnapDrive für UNIX und SnapManager ausgeführt
    - Sekundäre Storage-Systeme
    - DataFabric Manager Server
  - **Installierte Produkte**

    Für dieses Beispiel müssen die folgenden Lizenzen auf diesen Systemen aktiviert sein:

    - Data ONTAP 7.3.1 oder höher
    - SnapVault ONTAP Primärspeicher
    - FlexVol (erforderlich für NFS)
    - SnapRestore
    - NFS-Protokoll
- **TechCo Sekundärspeichersysteme**

  Die sekundären Storage-Systeme an einem über das Netzwerk verbundenen sekundären Storage-Standort, sind 50 Meilen entfernt, und speichern sekundäre Backups der Gehaltsabrechnungsdatenbank.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügen die sekundären Speichersysteme über Netzwerkverbindungen mit den folgenden Komponenten:

    - Primärspeicher
    - DataFabric Manager Server
  - **Installierte Produkte**

    In diesem Beispiel müssen die folgenden Lizenzen auf den sekundären Speichersystemen aktiviert sein:

    - Data ONTAP
    - SnapVault ONTAP Sekundärspeicher

        - SnapRestore
        - FlexVol (erforderlich für NFS)
        - NFS-Protokoll
- **DataFabric Manager Server**

  Der DataFabric Manager Server, techco_dfm, befindet sich an der Unternehmenszentrale an einem Standort, auf den der Storage-Administrator zugreifen kann. DataFabric Manager Server koordiniert unter anderem die Backup-Aufgaben zwischen dem primären und dem sekundären Storage.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes unterhält der DataFabric Manager Server Netzwerkverbindungen mit den folgenden Komponenten:

    - NetApp Management Console
    - Primärspeicher
    - Sekundäre Storage-Systeme
  - **Installierte Produkte**

    Der DataFabric Manager-Server ist für die folgenden Serverprodukte für dieses Beispiel lizenziert:

    - DataFabric Manager
- **SnapManager-Repository**

  Das SnapManager-Repository auf einem dedizierten Server speichert Daten zu den von SnapManager ausgeführten Vorgängen, beispielsweise zum Zeitpunkt von Backups, Tabellen und Datendateien, die gesichert wurden, von verwendeten Storage-Systemen, erstellten Klonen und von Snapshot Kopien. Wenn ein DBA eine vollständige oder teilweise Wiederherstellung versucht, fragt SnapManager das Repository ab, um von SnapManager für Oracle zur Wiederherstellung erstellte Backups zu identifizieren.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügen die sekundären Speichersysteme über Netzwerkverbindungen mit den folgenden Komponenten:

    - SnapManager Host
    - SnapManager für Oracle Client
- **NetApp Management Console**

  Die NetApp Management Console ist die grafische Benutzeroberfläche, über die der Storage-Administrator Zeitpläne, Richtlinien, Datensätze und Ressourcen-Pool-Zuweisungen konfiguriert, um Backups in sekundären Storage-Systemen zu ermöglichen, auf die der Storage-Administrator zugreifen kann.

  - **Verbindungen**

    Zur Unterstützung des sekundären Backup-Schutzes verfügt die NetApp Management Console über Netzwerkverbindungen mit den folgenden Komponenten:

    - Primärspeicher
    - Sekundäre Storage-Systeme

        - DataFabric Manager Server
- **SnapManager für Oracle-Client**

  Der SnapManager für Oracle Client ist die grafische Benutzeroberfläche und Befehlszeilenkonsole, die von dem DBA für die Gehaltsabrechnungsdatenbank in diesem Beispiel für die Konfiguration und das Durchführen eines lokalen Backups und Backups im Sekundärspeicher verwendet wird.

  - **Verbindungen**

    Zur Unterstützung von lokalem Backup und sekundärem Backup-Schutz verfügt SnapManager für den Oracle Client über Netzwerkverbindungen mit den folgenden Komponenten:

    - SnapManager Host
    - SnapManager-Repository für Datenbanken, SnapDrive für UNIX und SnapManager
    - Datenbank-Host (wenn getrennt von dem Host, auf dem SnapManager ausgeführt wird)
    - DataFabric Manager Server
  - **Installierte Produkte**

    Zur Unterstützung von lokalem Backup und sekundärem Backup-Schutz muss die SnapManager für Oracle Client-Software auf dieser Komponente installiert sein.

Backup-Zeitplan und Aufbewahrungsstrategie

Der DBA möchte sicherstellen, dass Backups im Falle eines Datenverlusts, im Fall eines Notfalls und aus gesetzlichen Gründen verfügbar sind. Dies erfordert eine sorgfältig durchdachte Aufbewahrungsrichtlinie für die verschiedenen Datenbanken.

Bei der Gehaltsabrechnungsdatenbank für die Produktion hält sich der DBA an die folgende TechCo-Aufbewahrungsstrategie:

Sicherungshäufigkeit	Aufbewahrungsdauer	Backup-Zeit	Art des Storage
Einmal täglich	10 Tage	7 Uhr	Primär (lokal)
Einmal täglich	10 Tage	7 Uhr	Sekundär (Archiv)
Einmal pro Woche	52 Wochen	Samstags 1 Uhr	Sekundär (Archiv)

- **Vorteile der lokalen Sicherung**

  Die täglichen lokalen Backups bieten sofortige Datenbanksicherung, belegt keine Netzwerkbandbreite, benötigt minimalen zusätzlichen Speicherplatz, ermöglicht die sofortige Wiederherstellung und bietet fein abgestimmte Backup- und Restore-Funktionen.

  Da die letzten wöchentlichen Backups der Gehaltsabrechnungsdatenbank für mindestens 52 Wochen an einem sekundären Standort aufbewahrt werden, müssen die täglichen Backups nicht mehr als 10 Tage aufbewahrt werden.

- **Geschützte Backup-Vorteile**

Tägliche und wöchentliche Backups auf dem Sekundärspeicher an einem Remote-Standort gewährleisten, dass die Zieldatenbank weiterhin gesichert ist und aus dem Sekundärspeicher wiederhergestellt werden kann, wenn die Daten am primären Storage-Standort beschädigt sind.

Die täglichen Backups auf dem Sekundärspeicher werden durchgeführt, um das System vor Schäden am primären Speichersystem zu schützen. Da die letzten wöchentlichen Backups der Gehaltsabrechnungsdatenbank für mindestens 52 Wochen aufbewahrt werden, muss die tägliche Sicherung nicht mehr als 10 Tage aufbewahrt werden.

Workflow-Zusammenfassung für lokale und sekundäre Datenbank-Backups

In diesem Beispiel koordinieren der DBA (mittels SnapManager) und der Storage-Administrator (mithilfe der Datensicherheitsfunktion der NetApp Management Console) Aktionen zur Konfiguration von lokalem Backup und sekundärem Backup (auch als geschütztes Backup bezeichnet) der Zieldatenbank.

Die Reihenfolge der durchgeführten Maßnahmen ist wie folgt zusammengefasst:

- **Konfiguration des sekundären Ressourcen-Pools**

  Der Storage-Administrator konfiguriert mithilfe der Datensicherheitsfunktion der NetApp Management Console einen Ressourcen-Pool aus Storage-Systemen am sekundären Standort, der zum Speichern des Gehaltsabrechnungs-Backups verwendet werden kann.

- **Sekundärsicherungsplan**

  Der Storage-Administrator konfiguriert mithilfe der Datensicherheitsfunktion der NetApp Management Console sekundäre Backup-Zeitpläne.

- **Konfiguration der Schutzrichtlinien**

  Der Storage-Administrator konfiguriert mithilfe der Datensicherungsfunktionen der NetApp Management Console eine sekundäre Backup-Sicherungsrichtlinie für die Zieldatenbank. Die Sicherungsrichtlinie umfasst die Zeitpläne und legt den Basistyp für die Implementierung von Backup-Sicherung (Backup, Spiegelung oder Kombination aus beidem) fest sowie Richtlinien zur Aufbewahrung von Primärdaten, sekundären und manchmal tertiären Storage Nodes.

- **Zuweisung von Datenbankprofilen und Schutzrichtlinien**

  Der DBA erstellt und bearbeitet mit SnapManager ein Profil der Zieldatenbank, die das sekundäre Backup unterstützt. Beim Konfigurieren des Profils verfügt der DBA über:

  - Ermöglicht Backup-Sicherung auf sekundärem Storage.
  - Weist diesem Profil die neue Sicherungsrichtlinie zu, die in erstellt wurde und von der Datensicherungsfunktion der NetApp Management Console abgerufen wurde.

    Das Zuweisen der Sicherungsrichtlinie schließt die Zieldatenbank automatisch in einem teilweise bereitgestellten, nicht jedoch den Datensatz mit der Datensicherungsfunktion der NetApp Management Console ein. Wenn die Datensatzkonfiguration vollständig bereitgestellt ist, kann das Backup der Zieldatenbank auf dem sekundären Storage aktiviert werden.

  Der Datensatz-Name verwendet diese Syntax: smo_hostname_databaseame, was sich in „smo_payroll.techco.com_paydb"“ übersetzt.

- **Sekundäre und tertiäre Speicherbereitstellung**

  Der Storage-Administrator nutzt die NetApp Management Console Datensicherungsfunktionen, um Ressourcen-Pools zuzuweisen, um sekundäre und manchmal tertiäre Storage Nodes bereitzustellen (wenn in der zugewiesenen Sicherungsrichtlinie tertiäre Storage Nodes angegeben sind).

- **Backup auf lokalem Speicher**

  Der DBA öffnet das Profil mit aktiviertem Schutz in SnapManager und erstellt eine vollständige Sicherung zum lokalen Speicher. Das neue Backup wird in SnapManager als geplant für die Sicherung angezeigt, aber noch nicht geschützt.

- **Sekundäre Backup-Bestätigung**

  Da das Backup auf einem schutzfähigen Profil basiert, wird das Backup gemäß dem Zeitplan der Sicherungsrichtlinie auf einen zweiten übertragen. Der DBA bestätigt die Übertragung des Backups auf den sekundären Storage mithilfe von SnapManager. Nachdem das Backup in den sekundären Storage kopiert wurde, ändert SnapManager den Sicherungsstatus von „nicht geschützt“ in „geschützt“.

Geschützte Backup-Konfiguration und -Ausführung

Sie müssen SnapManager und Protection Manager konfigurieren, um die Datenbank-Sicherung auf dem sekundären Storage zu unterstützen. Der Datenbank-Administrator und der Storage-Administrator müssen ihre Aktionen koordinieren.

Verwenden von SnapManager für Oracle, um das Datenbankprofil für ein lokales Backup zu erstellen

Die Datenbankadministratoren erstellen mithilfe von SnapManager ein Datenbankprofil, mit dem ein Backup im lokalen Storage eines primären Storage-Systems initiiert wird. Die gesamte Profilerstellung und Backup-Erstellung werden in SnapManager vollständig durchgeführt – einschließlich Protection Manager ist also nicht erforderlich.

Ein Profil enthält die Informationen über die zu verwaltende Datenbank, einschließlich der Anmeldeinformationen, Backup-Einstellungen und Sicherungseinstellungen für Backups. Wenn Sie ein Profil erstellen, müssen Sie bei jeder Operation in dieser Datenbank keine Datenbankdetails angeben, sondern nur den Profilnamen angeben. Ein Profil kann nur auf eine Datenbank verweisen. Auf dieselbe Datenbank kann von mehr als einem Profil verwiesen werden.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Klicken Sie in der Struktur SnapManager-Repositories mit der rechten Maustaste auf den Host, der mit diesem Profil verknüpft werden soll, und wählen Sie **Profil erstellen** aus.
3. Geben Sie auf der Seite Profilkonfigurationsinformationen die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - Profilname: Gehaltsabrechnung_Prod
   - Profilpasswort: Payrol123
   - Kommentar: Production Payroll Datenbank
4. Geben Sie auf der Seite Datenbankkonfigurationsinformationen die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - Datenbankname: PAYDB

- Datenbank-SID: Payrolldb
- Datenbank-Host: Standard akzeptieren

  Da Sie ein Profil von einem Host in der Repository-Struktur erstellen, zeigt SnapManager den Hostnamen an.

5. Akzeptieren Sie auf der zweiten Seite Datenbankkonfigurationsinformationen die folgenden Datenbankinformationen und klicken Sie auf **Weiter**:
   - Host-Konto, Vertretung des Oracle-Benutzerkontos: oracle
   - Host-Gruppe, die die Oracle-Gruppe repräsentiert: dba
6. Wählen Sie auf der Seite Datenbankverbindungsinformationen die Option **Datenbankauthentifizierung verwenden** aus, damit Benutzer sich mit Datenbankinformationen authentifizieren können.

   Geben Sie für dieses Beispiel die folgenden Informationen ein und klicken Sie auf **Weiter**.

   - SYSDBA Privileged User Name, der den Systemadministrator der Systemdatenbank repräsentiert, der über Administratorrechte verfügt: Sys
   - Kennwort (SYSDBA-Kennwort): oracle
   - Port zur Verbindung mit Datenbank-Host: 1521
7. Wählen Sie auf der Seite RMAN-Konfigurationsinformationen die Option **nicht RMAN verwenden** aus, und klicken Sie auf **Weiter**.

   Oracle Recovery Manager (RMAN) ist ein Oracle Tool für das Backup und Recovery von Oracle Datenbanken mithilfe der Erkennung auf Blockebene.

8. Geben Sie auf der Seite Snapshot Naming Information eine Namenskonvention für die mit diesem Profil verknüpften Snapshots an, indem Sie Variablen auswählen. Die einzige Variable, die benötigt wird, ist die **smid**-Variable, die eine eindeutige Snapshot-Kennung erstellt.

   Gehen Sie in diesem Beispiel wie folgt vor:

   a. Wählen Sie in der Liste Variable Token die Variable **{usertext}** aus und klicken Sie auf **Hinzufügen**.
   b. Geben Sie „payroll.techco.com_" als Host-Name ein und klicken Sie auf **OK**.
   c. Klicken Sie auf **links**, bis der Hostname kurz nach "Smo" im Feld Format angezeigt wird.
   d. Klicken Sie Auf **Weiter**.

   Die Snapshot Namenskonvention von smo_hostname_smoprofile_dbsid_scope_Mode_smid wird „smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (wo der „f“ ein vollständiges Backup anzeigt, das „A“ den automatischen Modus angibt, und das „x“ stellt den einzigartigen SMID dar).

9. Überprüfen Sie auf der Seite Vorgang durchführen die Informationen und klicken Sie auf **Erstellen**.
10. Klicken Sie auf **Operation Details**, um Informationen über den Vorgang zum Erstellen von Profilen und zur Volume-basierten Wiederherstellung anzuzeigen.

Konfigurieren eines sekundären Ressourcen-Pools mit Protection Manager

Um das Backup der Datenbank auf dem sekundären Storage zu unterstützen, verwendet der Storage-Administrator Protection Manager, um die sekundären Storage-Systeme, die mit der sekundären SnapVault-Lizenz aktiviert sind, in einem Ressourcen-Pool für die

Backups zu organisieren.

Idealerweise können Storage-Systeme in einem Ressourcen-Pool mit Blick auf ihre Akzeptanz als Ziele für Backups ausgetauscht werden. Wenn Sie zum Beispiel die Sicherungsstrategie für die Gehaltsabrechndatenbank entwickeln, identifizierten Sie als Storage-Administrator sekundäre Storage-Systeme mit einer ähnlichen Performance und Servicequalität, die als Mitglieder desselben Ressourcen-Pools geeignet wären.

Sie haben bereits Aggregate mit ungenutztem Speicherplatz auf Storage-Systemen erstellt, die Sie Ressourcen-Pools zuweisen möchten. Dadurch wird sichergestellt, dass ausreichend Platz zum Einhalten der Backups vorhanden ist.

1. Gehen Sie zur NetApp Management Console des Protection Manager.
2. Klicken Sie in der Menüleiste auf **Daten** > **Ressourcen-Pools**.

   Das Fenster Ressourcen-Pools wird angezeigt.

3. Klicken Sie Auf **Hinzufügen**.

   Der Assistent zum Hinzufügen von Ressourcen-Pools wird gestartet.

4. Führen Sie die Schritte im Assistenten aus, um den Ressourcen-Pool **paydb_Backup_Resource** zu erstellen.

   Verwenden Sie folgende Einstellungen:

   - Name: Verwenden Sie **paydb-Backup_Resource**
   - Speicherplatzschwellenwerte (verwenden Sie die Standardeinstellungen):
     - Schwellenwerte für die Speicherplatzauslastung: Aktiviert
     - Schwellenwert fast erreicht (für Ressourcenpool): 80 %
     - Schwellenwert (für Ressourcenpool): 90 %

Mit Protection Manager können Sie sekundäre Backup-Pläne konfigurieren

Um das Backup der Datenbank auf dem sekundären Storage zu unterstützen, verwendet der Storage-Administrator Protection Manager zum Konfigurieren eines Backup-Zeitplans.

Vor der Konfiguration des Zeitplans für sekundäre Backups gibt der Storage-Administrator folgende Informationen mit dem DBA-Partner:

- Den Zeitplan, den der DBA die sekundären Backups befolgen möchte.

  In diesem Fall finden einmal täglich Sicherungen um 7 Uhr statt Und einmal wöchentlich erfolgen Backups samstags um 1 Uhr

  a. Wechseln Sie zur NetApp Management-Konsole des Protection Manager.
  b. Klicken Sie in der Menüleiste auf **Richtlinien** > **Schutz** > **Zeitpläne**.

     Die Registerkarte Zeitpläne im Fenster Schutzrichtlinien wird angezeigt.

  c. Wählen Sie in der Terminliste den Tagesplan**täglich um 8:00 Uhr** aus.

d. Klicken Sie Auf **Kopieren**.

   Ein neuer Tagesplan, **Kopie des Tages um 8:00 Uhr**, wird in der Liste angezeigt. Sie ist bereits ausgewählt.

e. Klicken Sie Auf **Bearbeiten**.

   Die Eigenschaftenblatt „Tagesplan bearbeiten“ wird auf der Registerkarte „Zeitplan“ geöffnet.

f. Ändern Sie den Terminplannamen um 7 Uhr auf **Payroll Daily**, aktualisieren Sie die Beschreibung und klicken Sie dann auf **Apply**.

   Ihre Änderungen werden gespeichert.

g. Klicken Sie auf die Registerkarte * Tagesereignisse*.

   Die aktuelle tägliche Backup-Zeit des Zeitplans liegt bei 8:00 Uhr Wird angezeigt.

h. Klicken Sie auf **Hinzufügen** und geben Sie **7:00 PM** in das neue Zeitfeld ein, und klicken Sie dann auf **Anwenden**.

   Die aktuelle tägliche Backup-Zeit des Zeitplans ist jetzt 7:00 Uhr

i. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Eigenschaftenblatt zu verlassen.

   Ihr neuer Tagesplan, **Payroll Daily um 7 Uhr**, wird in der Terminliste angezeigt.

j. Wählen Sie den Wochenplan**Sonntag um 8:00 Uhr plus täglich** in der Terminliste aus.

k. Klicken Sie Auf **Kopieren**.

   Ein neuer Wochenplan, **Kopie des Sonntags um 8:00 Uhr plus täglich**, wird in der Liste angezeigt. Sie ist bereits ausgewählt.

l. Klicken Sie Auf **Bearbeiten**.

   Das Eigenschaftenblatt Wochenplan bearbeiten wird auf der Registerkarte Zeitplan geöffnet.

m. Ändern Sie den Terminplannamen in **Payroll Samstag um 1 UHR plus täglich um 7 Uhr** und aktualisieren Sie die Beschreibung.

n. Wählen Sie aus der Dropdown-Liste **Tagesplan** den soeben erstellten Tagesplan **Payroll Daily um 7 Uhr** aus.

   Wenn Sie **Payroll Daily um 7 Uhr** auswählen, wird in diesem Zeitplan festgelegt, wann der tägliche Betrieb stattfinden soll, wenn der **Gehaltsabrechnungsplan Samstag um 1 UHR plus täglich um 7 Uhr** auf eine Richtlinie angewendet wird.

o. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Eigenschaftenblatt zu verlassen.

   Ihr neuer Wochenplan, **Payroll Samstag um 1:00 Uhr plus täglich um 7:00 Uhr**, wird in der Terminliste angezeigt.

Konfigurieren einer sekundären Backup-Sicherungsrichtlinie mit Protection Manager

Nach der Konfiguration des Backup-Zeitplans konfiguriert der Storage-Administrator eine

geschützte Backup-Storage-Richtlinie, in die dieser Zeitplan aufgenommen werden soll.

Vor der Konfiguration der Schutzrichtlinie gibt der Storage-Administrator folgende Informationen an den DBA-Partner:

- Aufbewahrungsdauer zur Angabe für sekundären Storage
- Typ des erforderlichen sekundären Storage-Schutzes

Die Sicherungsrichtlinie, die erstellt wird, kann vom DBA-Partner in SnapManager für Oracle aufgelistet und einem Datenbankprofil für die zu sichernden Daten zugewiesen werden.

1. Gehen Sie zur NetApp Management Console des Protection Manager.
2. Klicken Sie in der Menüleiste auf **Richtlinien** > **Schutz** > **Übersicht**.

   Die Registerkarte Übersicht im Fenster Schutzrichtlinien wird angezeigt.

3. Klicken Sie auf **Richtlinie hinzufügen**, um den Assistenten zum Hinzufügen von Schutzrichtlinien zu starten.
4. Führen Sie den Assistenten mit den folgenden Schritten aus:

   a. Geben Sie einen beschreibenden Richtliniennamen an.

      Geben Sie in diesem Beispiel **TechCo Payroll Data: Backup** und eine Beschreibung ein und klicken Sie dann auf **Next**.

   b. Wählen Sie eine Basisrichtlinie aus.

      Wählen Sie für dieses Beispiel **Sichern** aus und klicken Sie auf **Weiter**.

   c. Akzeptieren Sie im Eigenschaftenblatt Richtlinie für den primären Datenknoten die Standardeinstellungen und klicken Sie auf **Weiter**.

      In diesem Beispiel wird der in SnapManager konfigurierte lokale Backup-Zeitplan angewendet. Jeder lokale Backup-Zeitplan, der mit dieser Methode angegeben wird, wird ignoriert.

   d. Wählen Sie im Eigenschaftenblatt primäre Daten zu Sicherungsverbindung einen Backup-Zeitplan aus.

      Wählen Sie in diesem Beispiel **Payroll Samstag um 1 UHR plus täglich um 7 Uhr** als Backup-Zeitplan aus und klicken Sie dann auf **Weiter**.

      In diesem Beispiel enthält der ausgewählte Zeitplan sowohl die wöchentlichen als auch die täglichen Zeitpläne, die Sie zuvor konfiguriert haben.

   e. Geben Sie im Eigenschaftenblatt Backup Policy den Namen des Backup-Knotens und die Aufbewahrungszeiten für tägliche, wöchentliche oder monatliche Backups an.

      Geben Sie in diesem Beispiel eine tägliche Backup-Aufbewahrung von 10 Tagen und eine wöchentliche Backup-Aufbewahrung von 52 Wochen an. Klicken Sie nach dem Ausfüllen jedes Eigenschaftenblatts auf **Weiter**.

   Nachdem alle Eigenschaftenblätter abgeschlossen sind, zeigt der Assistent zum Hinzufügen von Schutzrichtlinien eine Zusammenfassung für die Schutzrichtlinie an, die Sie erstellen möchten.

5. Klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Die **TechCo Payroll Data: Backup** Protection Policy ist unter den anderen Richtlinien für Protection Manager aufgelistet.

Der DBA-Partner kann nun mit SnapManager für Oracle diese Richtlinie auflisten und zuweisen, wenn das Datenbankprofil für die zu sichernden Daten erstellt wird.

Verwenden von SnapManager für Oracle, um das Datenbankprofil zu erstellen und eine Sicherungsrichtlinie zuzuweisen

Sie müssen in SnapManager für Oracle ein Profil erstellen, den Schutz im Profil aktivieren und eine Sicherungsrichtlinie zuweisen, um ein geschütztes Backup zu erstellen.

Ein Profil enthält Informationen über die zu verwaltende Datenbank, einschließlich der Anmeldeinformationen, Backup-Einstellungen und Sicherungseinstellungen für Backups. Nachdem Sie ein Profil erstellt haben, müssen Sie bei jedem Vorgang keine Datenbankdetails angeben. Ein Profil kann nur auf eine Datenbank verweisen, auf die dieselbe Datenbank kann jedoch mehrere Profile verweisen.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Klicken Sie in der Verzeichnisstruktur Repositories mit der rechten Maustaste auf den Host, und wählen Sie **Profil erstellen**.
3. Geben Sie auf der Seite Profilkonfigurationsinformationen die Profildetails ein, und klicken Sie auf **Weiter**.

   Sie können die folgenden Informationen eingeben:

   - Profilname: Payroll_prod2
   - Profilpasswort: Payrol123
   - Kommentar: Production Payroll Datenbank
4. Geben Sie auf den Seiten Datenbankkonfigurationsinformationen die Datenbankdetails ein, und klicken Sie auf **Weiter**.

   Sie können die folgenden Informationen eingeben:

   - Datenbankname: PAYDB
   - Datenbank-SID: Payrolldb
   - Datenbank-Host: Standard akzeptieren. Da Sie ein Profil von einem Host in der Repository-Struktur erstellen, zeigt SnapManager den Hostnamen an.
   - Host-Konto, Vertretung des Oracle-Benutzerkontos: oracle
   - Host-Gruppe, die die Oracle-Gruppe repräsentiert: dba
5. Klicken Sie auf der Seite Datenbankverbindungsinformationen auf **Datenbankauthentifizierung verwenden**, um Benutzern die Authentifizierung anhand von Datenbankinformationen zu ermöglichen.
6. Geben Sie die Daten zur Datenbankverbindung ein und klicken Sie auf **Weiter**.

   Sie können die folgenden Informationen eingeben:

   - SYSDBA Privileged User Name, der den Systemadministrator der Systemdatenbank repräsentiert, der über Administratorrechte verfügt: Sys

- Kennwort (SYSDBA-Kennwort): oracle
- Port zur Verbindung mit Datenbank-Host: 1521

7. Klicken Sie auf der Seite RMAN-Konfigurationsinformationen auf **nicht RMAN verwenden** und klicken Sie auf **Weiter**.

   Oracle Recovery Manager (RMAN) ist ein Oracle Tool für das Backup und Recovery von Oracle Datenbanken mithilfe der Erkennung auf Blockebene.

8. Geben Sie auf der Seite Snapshot Naming Information eine Namenskonvention für die mit diesem Profil verknüpften Snapshots an, indem Sie Variablen auswählen.

   Die smid-Variable erstellt eine eindeutige Snapshot-ID.

   Führen Sie Folgendes aus:

   a. Wählen Sie in der Liste Variable Token den Benutzertext aus und klicken Sie auf **Hinzufügen**.
   b. Geben Sie payroll.techco.com_ als Host-Name ein und klicken Sie auf **OK**.
   c. Klicken Sie auf **links**, bis der Hostname kurz nach dem Smo im Feld Format angezeigt wird.
   d. Klicken Sie Auf **Weiter**.

   Die Snapshot Namenskonvention von smo_hostname_smoprofile_dbsid_scope_Mode_smid wird „smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (wo „f“ auf ein vollständiges Backup hinweist, „A“ den automatischen Modus angibt, und „x“ stellt den einzigartigen SMID dar).

9. Wählen Sie **Protection Manager Protection Policy** Aus.

   Mit der **Protection Manager Protection Policy** können Sie eine Schutzrichtlinie auswählen, die mithilfe der NetApp Management Console konfiguriert wurde.

10. Wählen Sie aus den Schutzrichtlinien der NetApp Management Console **TechCo Payroll Data: Backup** aus und klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite Vorgang durchführen die Informationen und klicken Sie auf **Erstellen**.
12. Klicken Sie auf **Operation Details**, um Informationen über den Vorgang zum Erstellen von Profilen und zur Volume-basierten Wiederherstellung anzuzeigen.
    - Die Zuweisung einer NetApp Management Console Sicherungsrichtlinie für das Datenbankprofil erstellt automatisch einen nicht konformen Datensatz, der für den NetApp Management Console Operator sichtbar ist. Dabei wird der Name convention smo_<hostname>_<profilname> oder in diesem Beispiel: smo_payroll.tech.com_PAYDB angegeben.
    - Falls das Profil nicht für die Wiederherstellung von Volumes geeignet ist (auch als „schnelle Wiederherstellung“ bezeichnet), geschieht Folgendes:
      - Die Registerkarte **Ergebnisse** zeigt an, dass die Profilerstellung erfolgreich war und dass während des Vorgangs Warnungen aufgetreten sind.
      - Die Registerkarte **Operation Details** enthält ein WARNPROTOKOLL, in dem angegeben wird, dass das Profil nicht für eine schnelle Wiederherstellung geeignet ist und warum.

Verwenden von Protection Manager, um den neuen Datensatz bereitzustellen

Nachdem der smo_paydb-Datensatz erstellt wurde, verwendet der Storage-Administrator Protection Manager, um Storage-System-Ressourcen zuzuweisen, um den Backup-Node des Datensatzes bereitzustellen.

Vor dem Bereitstellen des neu erstellten Datensatzes vergibt der Storage-Administrator den Namen des im Profil angegebenen Datensatzes mit dem DBA-Partner.

In diesem Fall lautet der Datensatzname smo_payroll.tech.com_PAYDB.

1. Gehen Sie zur NetApp Management Console des Protection Manager.
2. Klicken Sie in der Menüleiste auf **Daten** > **Datensätze** > **Übersicht**.

   Auf der Registerkarte „Datensätze“ des Fensters „Datensätze“ wird eine Liste mit Datensätzen angezeigt, zu denen auch der Datensatz gehört, der gerade über SnapManager erstellt wurde.

3. Suchen Sie den **smo_payroll.tech.com_PAYDB**-Datensatz und wählen Sie ihn aus.

   Wenn Sie diesen Datensatz auswählen, zeigt der Diagrammbereich den smo_paydb-Datensatz mit seinem Datensicherungs-Knoten nicht bereitgestellt an. Der Konformitätsstatus wird als nicht-konform gekennzeichnet.

4. Wenn der smo_paydb-Datensatz noch hervorgehoben ist, klicken Sie auf **Bearbeiten**.

   Die NetApp Management Console des Protection Manager zeigt das Datensatz-Fenster Bearbeiten für den **smo_payroll.tech.com_PAYDB** Datensatz an. Im Navigationsbereich des Fensters werden Konfigurationsoptionen für den primären Knoten des Datensatzes, die Sicherungsverbindung und den Backup-Knoten angezeigt.

5. Suchen Sie im Navigationsbereich die Optionen für den Backup-Knoten des Datensatzes und wählen Sie **Provisioning/Resource-Pools**.

   Im Fenster Datensatz bearbeiten wird eine Einstellung für die Standard-Provisionierungsrichtlinie und eine Liste verfügbarer Ressourcen-Pools angezeigt.

6. Wählen Sie für dieses Beispiel den Ressourcen-Pool **paydb_Backup_Resource** aus, und klicken Sie auf **>**.

   Der ausgewählte Ressourcen-Pool wird im Feld „Ressourcen-Pools für diesen Node“ aufgelistet.

7. Klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Der Protection Manager stellt den sekundären Backup-Knoten automatisch mit Ressourcen aus dem Paydb_Backup_Resource-Pool bereit.

Verwendung von SnapManager für Oracle zur Erstellung eines geschützten Backups

Bei der Erstellung eines Backups für dieses Beispiel wählt der DBA die Erstellung eines vollständigen Backups, die Einstellung von Backup-Optionen und die Auswahl des Schutzes auf dem sekundären Speicher aus. Obwohl das Backup zunächst auf einem lokalen Storage erstellt wird, da dieses Backup auf einem schutzfähigen Profil basiert, wird das Backup dann gemäß dem Zeitplan der Sicherungsrichtlinie wie in Protection Manager definiert auf Sekundär-Storage übertragen.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Klicken Sie im SnapManager Repository-Baum mit der rechten Maustaste auf das Profil, das die Datenbank enthält, die Sie sichern möchten, und wählen Sie **Backup** aus.

Der Backup-Assistent SnapManager für Oracle wird gestartet.

3. Geben Sie Production_Payroll als Beschriftung ein.
4. Geben Sie die Produktionsabrechnung Jan 19 Backup als Kommentar ein.
5. Wählen Sie als Backup-Typ die Option **Auto** aus, die Sie erstellen möchten.

   So kann SnapManager bestimmen, ob ein Online- oder Offline-Backup durchgeführt wird.

6. Wählen Sie **Daily** oder **Weekly** als Häufigkeit des Backups aus.
7. Um zu bestätigen, dass der Backup ein gültiges Format für Oracle hat, aktivieren Sie das Kontrollkästchen neben **Backup überprüfen**.

   Bei diesem Vorgang wird das Blockformat und die -Struktur mit Oracle DBVerify überprüft.

8. Um den Status der Datenbank in den entsprechenden Modus zu versetzen (z. B. von öffnen auf gemountet), wählen Sie **Start erlauben oder Herunterfahren der Datenbank, falls erforderlich**, und klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite Datenbank, Tablespaces oder Datafiles to Backup die Option **Full Backup** aus, und klicken Sie auf **Next**.
10. Um die Sicherung auf einem sekundären Speicher zu schützen, überprüfen Sie **Sichern Sie das Backup** und klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite Vorgang durchführen die von Ihnen bereitgestellten Informationen und klicken Sie auf **Sicherung**.
12. Zeigen Sie auf der Seite „Fortschritt“ den Fortschritt und die Ergebnisse der Backup-Erstellung an.
13. Um die Details der Operation anzuzeigen, klicken Sie auf **Betriebsdetails**.

Bestätigen Sie den Backup-Schutz mit SnapManager für Oracle

Mit SnapManager für Oracle können Sie eine Liste der mit einem Profil verknüpften Backups anzeigen, bestimmen, ob die Backups für den Schutz aktiviert wurden, und die Aufbewahrungsklasse (in diesem Beispiel täglich oder wöchentlich) anzeigen.

Zunächst wird das neue Backup in diesem Beispiel als geplant für den Schutz angezeigt, aber noch nicht geschützt (in der grafischen Benutzeroberfläche des SnapManager und in der Ausgabe des Backup show-Befehls). Nachdem der Storage-Administrator sicherstellt, dass das Backup in den sekundären Storage kopiert wurde, ändert SnapManager den Backup-Sicherungsstatus sowohl in der grafischen Benutzeroberfläche als auch mit dem Befehl der Backup-Liste von „nicht geschützt“ in „geschützt“.

1. Wechseln Sie zum SnapManager für Oracle Client.
2. Erweitern Sie in der Struktur des SnapManager-Repository das Profil, um seine Backups anzuzeigen.
3. Klicken Sie auf die Registerkarte **Backups/Klone**.
4. Wählen Sie im Fensterbereich Berichte die Option **Backup Details** aus.
5. Überprüfen Sie in der Spalte Schutz, und stellen Sie sicher, dass der Status „geschützt“ lautet.

Datenbankwiederherstellung aus Backup

Wenn der aktive Inhalt der Gehaltsabrechnungsdatenbank versehentlich verloren geht oder zerstört wird, unterstützen SnapManager und die Datensicherheitsfunktion der

NetApp Management Console die Wiederherstellung dieser Daten entweder aus einem lokalen Backup oder einem sekundären Storage.

Einsatz von SnapManager für Oracle zur Wiederherstellung eines lokalen Backups im Primärspeicher

Sie können lokale Backups, die sich im Primärspeicher befinden, wiederherstellen. Der gesamte Prozess wird mit SnapManager für Oracle durchgeführt.

Sie können auch eine Vorschau der Informationen zu einem Backup-Wiederherstellungsprozess anzeigen. Möglicherweise möchten Sie dies tun, um Informationen über die Berechtigung zur Wiederherstellung eines Backups anzuzeigen. SnapManager analysiert die Daten für ein Backup, um zu ermitteln, ob der Wiederherstellungsprozess mithilfe der Volume-basierten Wiederherstellung oder der dateibasierten Restore-Methode abgeschlossen werden kann.

In der Vorschau der Wiederherstellung werden die folgenden Informationen angezeigt:

- Welcher Wiederherstellungsmechanismus (schnelle Wiederherstellung, Filesystem-Wiederherstellung auf Storage-Seite, Dateiwiederherstellung auf Storage-Seite oder Wiederherstellung von Host-seitigen Dateikopien) wird zum Wiederherstellen jeder Datei verwendet.
- Warum effizientere Mechanismen nicht verwendet wurden, um jede Datei wiederherzustellen.

In der Vorschau des Wiederherstellungsplans, SnapManager nichts wiederherstellt. In der Vorschau werden Informationen von bis zu 20 Dateien angezeigt.

Wenn Sie eine Vorschau einer Wiederherstellung von Datendateien, aber die Datenbank ist nicht gemountet, dann SnapManager mountet die Datenbank. Wenn die Datenbank nicht gemountet werden kann, schlägt der Vorgang fehl und SnapManager gibt die Datenbank in ihren ursprünglichen Zustand zurück.

1. Klicken Sie in der Repository-Struktur mit der rechten Maustaste auf das Backup, das Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen** aus.
2. Klicken Sie auf der Startseite des Wiederherstellungs- und Wiederherstellungsassistenten auf **Weiter**.
3. Wählen Sie auf der Seite Konfigurationsinformationen wiederherstellen die Option **vollständige Datei/Tablespace Wiederherstellung mit Steuerdateien** aus.
4. Klicken Sie auf **Herunterfahren der Datenbank zulassen, falls erforderlich**.

   Falls erforderlich ändert SnapManager den Datenbankstatus. Wenn beispielsweise die Datenbank offline ist und sie online sein muss, erzwingt SnapManager sie online.

5. Klicken Sie auf der Seite Wiederherstellungskonfigurationsinformationen auf **Alle Protokolle**.

   SnapManager stellt die Datenbank für die letzte Transaktion wieder her und wendet alle erforderlichen Protokolle an.

6. Zeigen Sie auf der Seite Konfiguration des Quellenstandorts wiederherstellen die Informationen zum Backup auf dem primären Speicherort an, und klicken Sie auf **Weiter**.

   Wenn das Backup nur auf dem Primärspeicher besteht, stellt SnapManager das Backup aus dem Primärspeicher wieder her.

7. Wählen Sie auf der Seite mit den Informationen zur Volume-Wiederherstellung die Option **Versuch einer Volume-Wiederherstellung** aus, um die Methode zur Volume-Wiederherstellung zu versuchen.
8. Klicken Sie auf **Fallback to file-based restore**.

Dadurch kann SnapManager die dateibasierte Wiederherstellungsmethode verwenden, wenn die Wiederherstellungsmethode des Volumes nicht verwendet werden kann.

9. Klicken Sie auf **Vorschau**, um die Eignungsprüfungen für schnelle Wiederherstellung und Informationen zu obligatorischen und überfrierbaren Prüfungen anzuzeigen.
10. Überprüfen Sie auf der Seite Vorgang durchführen die eingegebenen Informationen und klicken Sie auf **Wiederherstellen**.
11. Um Details zum Prozess anzuzeigen, klicken Sie auf **Betriebsdetails**.

Verwendung von SnapManager für Oracle zur Wiederherstellung von Backups aus dem sekundären Storage

Administratoren können geschützte Backups von sekundärem Storage wiederherstellen und wählen, wie die Daten zurück auf den primären Storage kopiert werden sollen.

Bevor Sie versuchen, das Backup wiederherzustellen, prüfen Sie die Backup-Eigenschaften und stellen Sie sicher, dass das Backup im primären Speichersystem freigegeben und auf dem Sekundärspeicher gesichert wird.

1. Klicken Sie in der Repository-Struktur SnapManager für Oracle mit der rechten Maustaste auf das Backup, das Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen** aus.
2. Klicken Sie auf der Startseite des Assistenten für Wiederherstellung und Wiederherstellung auf **Weiter**.
3. Klicken Sie auf der Seite Konfigurationsinformationen wiederherstellen auf **Datei/Tablespace Restore with Control Files**.
4. Klicken Sie auf **Herunterfahren der Datenbank zulassen, falls erforderlich**, und klicken Sie dann auf **Weiter**.

   Falls erforderlich ändert SnapManager den Datenbankstatus. Wenn beispielsweise die Datenbank offline ist und sie online sein muss, erzwingt SnapManager sie online.

5. Klicken Sie auf der Seite Wiederherstellungskonfigurationsinformationen auf **Alle Protokolle**. Klicken Sie anschließend auf **Weiter**.

   SnapManager stellt die Datenbank für die letzte Transaktion wieder her und wendet alle erforderlichen Protokolle an.

6. Wählen Sie auf der Seite Konfiguration des Quellenstandorts wiederherstellen die ID der geschützten Sicherungsquelle aus, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite „Konfigurationsinformationen zur Volume-Wiederherstellung“ auf **Versuch, die Volume-Wiederherstellung** zu starten, um die Volume-Wiederherstellung zu versuchen.
8. Klicken Sie auf **Fallback to file-based restore**.

   Dadurch kann SnapManager die dateibasierte Wiederherstellungsmethode verwenden, wenn die Wiederherstellungsmethode des Volumes nicht abgeschlossen werden kann.

9. Klicken Sie auf **Vorschau**, um die Eignungsprüfungen für schnelle Wiederherstellung und Informationen zu obligatorischen und überridbaren Prüfungen anzuzeigen.
10. Überprüfen Sie auf der Seite „Vorgang durchführen“ die von Ihnen bereitgestellten Informationen und klicken Sie auf **Wiederherstellen**.
11. Um Details zum Prozess anzuzeigen, klicken Sie auf **Betriebsdetails**.

Durchführung von Managementvorgängen

Sie können Managementaufgaben ausführen, nachdem Sie SnapManager eingerichtet und konfiguriert haben. Diese Aufgaben ermöglichen Ihnen das Management des normalen Betriebs, der über Backup, Wiederherstellung und Klonen hinaus geht.

Administratoren können Vorgänge entweder über die grafische Benutzeroberfläche oder über die Befehlszeilenschnittstelle ausführen.

Anzeigen einer Liste von Vorgängen

Sie können eine Zusammenfassung aller Vorgänge anzeigen, die für ein Profil durchgeführt wurden.

Sie können die folgenden Informationen anzeigen, wenn Sie Vorgänge auflisten, die einem bestimmten Profil zugeordnet sind:

- Start- und Enddatum bei Ausführung des Vorgangs
- Betriebsstatus
- Vorgangs-ID
- Art des Vorgangs
- Host, auf dem er ausgeführt wurde

a. Verwenden Sie den folgenden Befehl, um die Zusammenfassungsinformationen aller Vorgänge aufzulisten: `smo operation list profile -profile profile_name-delimiter character [-quiet | -verbose]`

   Wenn die Option -Trennzeichen angegeben wird, listet der Befehl jede Zeile in einer separaten Zeile auf und die Attribute in dieser Zeile werden durch das angegebene Zeichen getrennt.

Verwandte Informationen

Befehl smo Operation list

Anzeigen von Betriebsdetails

Sie können detaillierte Informationen zu einem bestimmten Profil anzeigen, um den Erfolg oder den Fehler einer Operation zu überprüfen. Zudem können Sie die verwendeten Storage-Ressourcen für einen bestimmten Vorgang ermitteln.

Sie können die folgenden Details zu einer bestimmten Operation anzeigen:

- Vorgangs-ID
- Art des Vorgangs
- Ob die Operation erzwungen wurde
- Laufzeitinformationen, einschließlich Status, Start- und Enddatum des Vorgangs
- Der Host, auf dem der Vorgang ausgeführt wurde, einschließlich der Prozess-ID und der SnapManager-Version

- Repository-Informationen
- Verwendete Storage-Ressourcen
  a. Um die detaillierten Informationen für eine bestimmte Vorgangs-ID anzuzeigen, geben Sie den folgenden Befehl ein: `smo operation show -profile profile_name [-label label | -id id] [-quiet | -verbose]`

Verwandte Informationen

Der Befehl smo Operation show

Befehle von einem alternativen Host ausgeben

Sie können CLI-Befehle von einem anderen Host als dem Datenbank-Host ausführen, und SnapManager führt die Befehle durch, die Sie an den entsprechenden Host eingeben.

Damit das System einen Vorgang an den richtigen Host sendet, muss es zunächst wissen, wo das Profil für den Vorgang gefunden werden soll. In diesem Verfahren speichert das System das Profil in Repository-Zuordnungsinformationen für eine Datei im Home-Verzeichnis des Benutzers auf dem lokalen Host.

1. Um das Home-Verzeichnis des lokalen Benutzers auf die Profile-zu-Repository-Zuordnungen aufmerksam zu machen, damit die Anforderung der Operation weiterleiten kann, geben Sie den folgenden Befehl ein: `smo profile sync -repository-dbname repo_dbname-host repo_host-port repo_port-login-username repo_username [-quiet | -verbose]`

Überprüfen der SnapManager-Softwareversion

Sie können ermitteln, welche Version des Produkts Sie auf Ihrem lokalen Host ausführen, indem Sie den Versionsbefehl ausführen.

1. Geben Sie zum Überprüfen der SnapManager-Version den folgenden Befehl ein: smo Version

Verwandte Informationen

Der Befehl smo Version

Beenden des SnapManager-Hostservers

Wenn Sie mit SnapManager fertig sind, möchten Sie den Server möglicherweise anhalten.

1. Geben Sie zum Beenden des Servers den folgenden Befehl als Root-Benutzer ein: `smo_server stop`

Verwandte Informationen

Der Befehl smo_Server stop

Starten Sie den SnapManager UNIX-Hostserver neu

Sie können den Server auf einem UNIX-Host mithilfe der CLI neu starten.

1. Geben Sie zum Neustart des Servers den folgenden Befehl ein: `smo_server restart`

Deinstallieren der Software von einem UNIX-Host

Wenn Sie die SnapManager-Software nicht mehr benötigen, können Sie sie auf dem Hostserver deinstallieren.

1. Melden Sie sich als Root an.
2. Geben Sie zum Beenden des Servers den folgenden Befehl ein: `smo_server stop`
3. Geben Sie zum Entfernen der SnapManager Software den folgenden Befehl ein: `UninstallSmo`
4. Drücken Sie nach dem Einführungstext **Enter**, um fortzufahren.

   Die Deinstallation ist abgeschlossen.

Verwandte Informationen

Der Befehl smo_Server stop

Konfigurieren einer E-Mail-Benachrichtigung

Mit SnapManager erhalten Sie eine E-Mail-Benachrichtigung über den Abschlussstatus der von den Profilen ausgeführten Datenbankvorgänge. SnapManager generiert die E-Mail und hilft Ihnen, entsprechend dem Status des Datenbankvorgangs entsprechende Maßnahmen zu ergreifen. Die Konfiguration der E-Mail-Benachrichtigung ist ein optionaler Parameter.

Sie können eine E-Mail-Benachrichtigung für ein einzelnes Profil als Profilbenachrichtigung und für mehrere Profile in einer Repository-Datenbank als zusammenfassende Benachrichtigung konfigurieren.

Profilbenachrichtigung

Für ein individuelles Profil können Sie eine E-Mail für erfolgreiche oder fehlerhafte Datenbankvorgänge erhalten.

Standardmäßig ist die E-Mail-Benachrichtigung für fehlgeschlagene Datenbankvorgänge aktiviert.

Zusammenfassende Benachrichtigung

Mit der Übersichtsbenachrichtigung erhalten Sie eine E-Mail über Datenbankvorgänge, die mit mehreren Profilen durchgeführt werden. Sie können stündliche, tägliche, wöchentliche oder monatliche Benachrichtigungen aktivieren.

Ab SnapManager 3.3 werden zusammenfassende Benachrichtigungen nur dann gesendet, wenn Sie den Hostserver angeben, der die Benachrichtigung senden soll. Wenn Sie SnapManager von einer Version vor 3.3 aktualisieren, werden die zusammenfassenden Benachrichtigungen möglicherweise nicht gesendet, wenn Sie den Host-Server in der Konfiguration für Übersichtsbenachrichtigungen nicht angegeben hatten.

Wenn Sie ein Repository in einem Knoten einer Datenbank erstellen, die sich in einer RAC-Umgebung (Real Application Clusters) befindet und eine zusammenfassende Benachrichtigung aktivieren, wird später, wenn Sie dasselbe Repository einem anderen Knoten der Datenbank hinzufügen, die E-Mail mit der Zusammenfassung zweimal gesendet.

Sie können Benachrichtigungen auf Profilebene oder eine zusammenfassende Benachrichtigung gleichzeitig verwenden.

SnapManager ermöglicht die E-Mail-Benachrichtigung für die folgenden profilausgeführten Datenbankvorgänge:

- Backup auf dem Primärspeicher
- Restore von Backups
- Erstellen von Klonen
- Split Clones
- Backup-Überprüfung

Nachdem Sie Profile mit aktivierter E-Mail-Benachrichtigung erstellt oder aktualisiert haben, können Sie sie deaktivieren. Wenn Sie die E-Mail-Benachrichtigung deaktivieren, erhalten Sie für diese profilausgeführten Datenbankvorgänge keine E-Mail-Benachrichtigungen mehr.

Die E-Mail, die Sie erhalten, enthält folgende Details:

- Name des Datenbankvorgangs, z. B. für Backup, Wiederherstellung oder Klonen
- Profilname, der für den Datenbankvorgang verwendet wird
- Name des Hostservers
- Systemkennung der Datenbank
- Start- und Endzeit des Datenbankvorgangs
- Status des Datenbankvorgangs
- Fehlermeldung, falls vorhanden
- Warnmeldungen, falls vorhanden

Sie können Folgendes konfigurieren:

- Mailserver für ein Repository
- E-Mail-Benachrichtigung für ein neues Profil
- E-Mail-Benachrichtigung für ein bestehendes Profil
- Zusammenfassende E-Mail-Benachrichtigung für mehrere Profile unter einem Repository

Sie können die E-Mail-Benachrichtigung sowohl über die Befehlszeilenschnittstelle (CLI) als auch über die grafische Benutzeroberfläche (GUI) konfigurieren.

Konfigurieren eines E-Mail-Servers für ein Repository

Mit SnapManager können Sie die E-Mail-Serverdetails angeben, von denen die E-Mail-Warnungen gesendet werden.

Mit SnapManager können Sie den Hostnamen oder die IP-Adresse des Absenders sowie die Portnummer des E-Mail-Servers für einen Repository-Datenbanknamen angeben, der eine E-Mail-Benachrichtigung erfordert. Sie können die Portnummer des Mail-Servers in einem Bereich von 0 bis 65535 konfigurieren; der Standardwert ist 25. Wenn Sie eine Authentifizierung für die E-Mail-Adresse benötigen, können Sie den Benutzernamen und das Kennwort angeben.

Sie müssen den Namen oder die IP-Adresse des Hostservers angeben, der die E-Mail-Benachrichtigung verarbeitet.

1. Um den E-Mail-Server zum Senden von E-Mail-Warnungen zu konfigurieren, geben Sie folgenden Befehl ein: bbs Notification Set -Sender-emailemail_address-mailhostmailhost-mailportmaiport [-Authentication-usernameusername-passwordpassword] -Repository-portrepo_Port-dbnamerepo_Service_Name -hostrepo_Host-Login-usernamernamerepo_username

   Weitere Optionen für diesen Befehl:

   [-Force]

Gehen Sie wie folgt vor:	Dann…
Um die E-Mail-Adresse des Absenders anzugeben.	Geben Sie die Option -Sender-E-Mail an. Unter SnapManager 3.2 für Oracle können Sie Bindestrich (-) einfügen, während Sie den Domain-Namen der E-Mail-Adresse angeben. Sie können beispielsweise die Absender-E-Mail-Adresse als -sender-emailuser@org-corp.com angeben.
Um den E-Mail-Server-Hostnamen oder die IP-Adresse des Absenders anzugeben.	Geben Sie die Option -mailhost an.
Zur Angabe der Port-Nummer des E-Mail-Servers für einen Repository-Datenbanknamen, der eine E-Mail-Benachrichtigung erfordert. Sie können die Portnummer des Mail-Servers in einem Bereich von null bis 65535 konfigurieren; der Standardwert ist 25.	Geben Sie die Option -mailport an.
Geben Sie den Benutzernamen und das Passwort an, wenn Sie eine Authentifizierung für die E-Mail-Adresse benötigen.	Geben Sie die Option -Authentication an, gefolgt vom Benutzernamen und Passwort.

Im folgenden Beispiel wird der Mail-Server konfiguriert.

```
smo notification set -sender-email admin1@org.com -mailhost
hostname.org.com -mailport 25 authentication -username admin1 -password
admin1 -repository -port 1521 -dbname SMOREPO -host hotspur -login
-username grabal21 -verbose
```

Konfigurieren der E-Mail-Benachrichtigung für ein neues Profil

Wenn Sie ein neues Profil erstellen, können Sie so konfigurieren, dass Sie eine E-Mail-Benachrichtigung nach Abschluss des Datenbankvorgangs erhalten.

- Sie müssen die E-Mail-Adresse konfigurieren, von der die Meldungen gesendet werden.
- Sie müssen eine kommagetrennte Liste für mehrere E-Mail-Adressen verwenden.

  Sie müssen sicherstellen, dass zwischen Komma und der nächsten E-Mail-Adresse kein Leerzeichen vorhanden ist.

  a. Geben Sie den folgenden Befehl ein: smo-Profil create -profileprofil [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port -Login-usernamerepo_username-commentation [-commosmany {] [-assogmgmgmnmail {] [-bussnmaimgmgninto} }] [-bussnmaimgmsmany [-bussninto] [-buttninto] [-buttnmgmgmsmany-adym] [-buttninto] [-assail] [-assail] [-assym] [-buttnmainto] [-bugmgmgmgmgmgmgmgmsmany [-buttnectionmsmany [-condo] [-bugmsmany-contactnmgmgmsmany [-condo] [-bug

  Weitere Optionen für diesen Befehl:

  [-Force]

  SnapManager unterstützt bis zu 1000 Zeichen für E-Mail-Adressen.

  Wenn Sie mithilfe des Profils (zur Erstellung separater Archiv-Log-Backups) eine Sicherung von Datendateien und Archivprotokolldateien erstellen und die Erstellung der Datendatei-Sicherung fehlschlägt, wird die E-Mail-Benachrichtigung mit der Datensicherung als Operationname anstatt Datensicherung und Archivprotokolle als Backup gesendet. Wenn die Datensicherung der Datendatei und der Archivprotokolldatei erfolgreich ist, wird die Ausgabe wie folgt angezeigt:

```
Profile Name    : PROF_31
Operation Name  : Data Backup and Archive Logs Backup
Database SID    : TENDB1
Database Host    : repo1.rtp.org.com
Start Date      : Fri Sep 23 13:37:21 EDT 2011
End Date          : Fri Sep 23 13:45:24 EDT 2011
Status          : SUCCESS
Error messages  :
```

Im folgenden Beispiel wird die E-Mail-Benachrichtigung angezeigt, die beim Erstellen eines neuen Profils konfiguriert wurde:

```
smo profile create -profile sales1 -profile-password sales1 -repository
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username oba5
-database -dbname DB1 -host 10.72.197.142 -sid DB1 -osaccount oracle
-osgroup dba -notification -success -email admin1@org.com -subject
{profile}_{operation-name}_{db-sid}_{db-host}_{start-date}_{end-
date}_{status}
```

Anpassen des E-Mail-Betreff für ein neues Profil

Sie können den E-Mail-Betreff für das neue Profil anpassen, wenn Sie es erstellen.

Sie können den Betreff der E-Mail mithilfe des {profile}_{Operation-Name}_{db-sid}_{db-Host}_{Startdatum}_{Enddatum}_{Status}-Musters anpassen oder Ihren eigenen Text eingeben.

Variablenname	Beschreibung	Beispielwert
Profil	Profilname, der für den Datenbankvorgang verwendet wird	PROF1
Operation-Name	Name des Datenbankvorgangs	Backup, Daten-Backup, Daten- und Archivprotokolle Backup
db-sid	SID der Datenbank	DB1
db-Host	Name des Hostservers	Hosta
Startdatum	Startzeit der Datenbankoperation im Format mmdd:hh:ss yyyy	April 27 21:00:45 PST 2012
Enddatum	Endzeit des Datenbankvorgangs im Format mmdd:hh:ss yyyy	April 27 21:10:45 PST 2012
Status	Status des Datenbankvorgangs	Erfolg

Wenn Sie keinen Wert für die Variablen angeben, zeigt SnapManager die folgende Fehlermeldung an: Missing value(s) -subject.

1. Geben Sie den folgenden Befehl ein: smo-Profil create -profileprofil [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port-Login-usernamerepo_username -commentation [-commosmany {] [-assogmnmaimgmninto {] [-countnmgname} }] [-durmsmany-contail] [-assail] [-butnmgmgmgmgmsbb] [-adym] [-buttnmnmnmnmnecimsmane] [-condo [-adym] [-bugmgmgmgmsmane] [-assainto [-condo] [-butnmaym [-butnmgmgmgmgmgmsmane] [-data] [-contactym] [-butnmgmgmgmgmn

Das folgende Beispiel zeigt das Muster des E-Mail-Betreff:

```
smo profile create -profile sales1 -profile-password admin1 -repository
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username admin2
-database -dbname DB1 -host 10.72.197.142 -sid DB1
-osaccount oracle -osgroup dba -profile-notification -success -email
admin@org.com -subject {profile}_{operation-name}_{db-sid}_{db-
host}_{start-date}_{end-date}_{status}
```

Konfigurieren der E-Mail-Benachrichtigung für ein vorhandenes Profil

Wenn Sie ein Profil aktualisieren, können Sie so konfigurieren, dass Sie eine E-Mail-Benachrichtigung über den Abschluss des Datenbankvorgangs erhalten.

- Sie müssen die E-Mail-Adresse konfigurieren, von der die Meldungen gesendet werden.
- Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die Benachrichtigungen gesendet werden.

  Sie können eine kommagetrennte Liste für mehrere Adressen verwenden. Sie müssen sicherstellen, dass zwischen Komma und der nächsten E-Mail-Adresse kein Leerzeichen vorhanden ist. Optional können Sie auch einen Betreff zu der E-Mail hinzufügen.

  a. Geben Sie den folgenden Befehl ein:smo-Profil-Update -profilprofil [-profile-passwordprofile_password][-Database-dbnamedb_dbname-Host db_Host [-siddb_sid] [-Login -usernamedb_username-adressyword-contail [-{] [-commentail] [-bosrimsrims2] [-commentail] [-] [-] [-] [-]]] [-assogmemassail] [-] [-{ commentail] [-{] [-] [-] [-]]] [-bosrimprotosrimnmaimnmailgms2}}}] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-commentail] [-] [-]] [-]] [-] [-] [-]]] [-]]]] [-commentail-]] [-] [-]

     Mit der Option Erfolg erhalten Sie nur eine Benachrichtigung für erfolgreiche Datenbankvorgänge und die Ausfalloption, eine Benachrichtigung nur für fehlerhafte Datenbankvorgänge zu erhalten.

Anpassen des E-Mail-Betreff für ein vorhandenes Profil

SnapManager ermöglicht Ihnen, das Muster des E-Mail-Betreff für ein bestehendes Profil anzupassen, indem Sie dieses Profil aktualisieren. Dieses benutzerdefinierte Muster für Studienteilnehmer gilt nur für das aktualisierte Profil.

1. Geben Sie den folgenden Befehl ein: smo-Profil-Update -profilprofil [-profile-passwordprofile_password][-Database-dbnamedb_dbname-Host db_Host [-siddb_sid] [-Login -usernamedb_username-adressyword -contail [-{] [-commentail] [-{ commentail-dnosrims2] [-{ commentail}}}] [-] [-] [-] [-]]]] [-assogame-commentail-bosrimpromnection[-] [-] [-] [-] [-] [-] [-] [-] [-]]]]] [-]]] [-assofundintosrimnoimnectumnectumprotos2] [-commented-commented-[-commmproperation[-] [-commgmn.jur-] [-] [-] [-] [-] [-] [

Das folgende Beispiel zeigt ein Muster für E-Mail-Betreff:

```
smo profile update -profile sales1 -profile-password sales1 -repository
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username admin2
-database -dbname DB1 -host 10.72.197.142 -sid DB1
-osaccount oracle -osgroup dba -profile-notification -success -email
admin@org.com -subject {profile}_{operation-name}_{db-sid}_{db-
host}_{start-date}_{end-date}_{status}
```

Konfigurieren einer E-Mail-Benachrichtigung mit Zusammenfassung für mehrere Profile

Mit SnapManager können Sie eine E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank konfigurieren.

Sie können den SnapManager-Server-Host als Benachrichtigungs-Host festlegen, von dem aus die zusammenfassende Benachrichtigung E-Mail an die Empfänger gesendet wird. Wenn der Hostname oder die IP-Adresse des SnapManager-Servers geändert wird, kann auch der Benachrichtigungs-Host aktualisiert werden.

Sie können eine der Zeitplanzeiten auswählen, zu denen Sie eine E-Mail-Benachrichtigung benötigen:

- Stündlich: Um jede Stunde eine E-Mail-Benachrichtigung zu erhalten
- Täglich: Um täglich eine E-Mail-Benachrichtigung zu erhalten
- Wöchentlich: Um wöchentlich eine E-Mail-Benachrichtigung zu erhalten
- Monatlich: Um monatlich eine E-Mail-Benachrichtigung zu erhalten

Sie müssen eine einzelne E-Mail-Adresse oder eine kommagetrennte Liste von E-Mail-Adressen eingeben, um Benachrichtigungen für Vorgänge zu erhalten, die mit diesen Profilen durchgeführt werden. Wenn Sie mehrere E-Mail-Adressen eingeben, müssen Sie sicherstellen, dass zwischen Komma und der nächsten E-Mail-Adresse kein Leerzeichen vorhanden ist.

SnapManager ermöglicht Ihnen das Hinzufügen eines benutzerdefinierten E-Mail-Betreff unter Verwendung der folgenden Variablen:

- Profilname, der für den Datenbankvorgang verwendet wird.
- Datenbankname
- SID der Datenbank
- Name des Hostservers
- Startzeit des Datenbankvorgangs im Format yyyymmdd:hh:ss
- Endzeit des Datenbankvorgangs im Format yyyyymmdd:hh:ss
- Status des Datenbankvorgangs

Wenn Sie kein angepasstes Thema hinzufügen möchten, zeigt SnapManager eine Fehlermeldung an: Missing value -subject.

1. Geben Sie folgenden Befehl ein: bbs Notification Update-summary-notification -Repository-portrepo_Port -dbnamerepo_Service_Name-hotropo_Host-Login-usernamerepo_username -emailemail_address1,email_address2-subject-pattern-frequency {-Daily-timedaily-time {4 7-31 5-3 6-

protagel1} {}} 1-wöchentlicher Hinweis

Weitere Optionen für diesen Befehl:

[-Force] [-noprompt]

```
smo notification update-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5 –email-address
admin@org.com –subject success –frequency -daily -time 19:30:45
–profiles sales1 -notification-host wales
```

Hinzufügen eines neuen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung

Nachdem Sie eine E-Mail-Benachrichtigung für die Repository-Datenbank konfiguriert haben, können Sie mithilfe des Befehls Summary Notification ein neues Profil zur zusammenfassenden Benachrichtigung hinzufügen.

1. Geben Sie den folgenden Befehl ein: smo-Profil create -profileprofile_Name [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port-Login -usernamerepo_username_countngmprop [-commosdbnum] [-admosmany-contactngname] [-assogmgn] [-composdn.jmgmgmgmgmgmgmgmgmgmgmgm-lep.jmgmgmgmgm.jm] [-{] [-budn.jmgmgmgmgmgmgmgmgmgmgmsdn.jmgmgmgmgmgmgmgmgmgmgm-data] [-{] [-butt.jmgmgmgmgmgmgmgm-data] [-} }-

   Weitere Optionen für diesen Befehl:

   [-Force]

Hinzufügen eines vorhandenen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung

Mit SnapManager können Sie ein vorhandenes Profil zu einer zusammengefassten E-Mail-Benachrichtigung hinzufügen und das Profil aktualisieren.

1. Geben Sie den folgenden Befehl ein: bbs-Profil-Update -profilprofile_Name [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port-Login -usernamerepo_username [-countmgardy] [-buttngmpromgstn.jmgmgmgm-lewym] [-assogm-lef_jm-datamn.jp.jm-datm-buttn.jmgmgm.jm-in.jpgmgm-in.j_jm-buttn.jm-butt.jmgmgm[-{ [-{] [-} }-buttnmgmgmgmgmgmgmgmgmgmgmgmgmgmgm-datamn.jm] [-Name [--buttn.jmgmgmgmgmgmgm-

Deaktivieren der E-Mail-Benachrichtigung für mehrere Profile

Nachdem Sie die E-Mail-Benachrichtigung für mehrere Profile aktiviert haben, können Sie sie deaktivieren, dass sie keine E-Mail-Benachrichtigungen mehr erhalten.

Mit SnapManager können Sie die E-Mail-Benachrichtigung mit der Zusammenfassung für diese profilausgeführten Datenbankvorgänge deaktivieren. Geben Sie über die SnapManager-CLI den Befehl

Benachrichtigung remove-summary-notification ein, um die Zusammenfassung der E-Mail-Benachrichtigung für mehrere Profile und den Namen der Repository-Datenbank zu deaktivieren, für die Sie keine E-Mail-Benachrichtigung benötigen.

1. Um die zusammenfassende Benachrichtigung für mehrere Profile in einer Repository-Datenbank zu deaktivieren, geben Sie den folgenden Befehl ein: smo notification remove-summary-notification -Repository-portrepo_Port-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username

Das folgende Beispiel zeigt, dass die zusammenfassende Benachrichtigung für mehrere Profile in einer Repository-Datenbank deaktiviert wird:

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5
```

Erstellen von Aufgabenspezifikationsdatei und Skripten für SnapManager-Vorgänge

SnapManager für Oracle verwendet eine XML-Datei (Extensible Markup Language) für die Aufgabenspezifikation, die Voraufgaben und Nachaufgaben für die Backup-, Wiederherstellungs- und Klonvorgänge anzeigt. Sie können die Skriptnamen vor und nach der Aufgabe in die XML-Datei einfügen, damit die Aufgaben vor oder nach den Backup-, Wiederherstellungs- und Klonvorgängen ausgeführt werden.

In SnapManager (3.1 oder früher) können Sie die Skripte für Voraufgabe und Nachaufgaben nur für den Klonvorgang ausführen. In SnapManager (3.2 oder höher) für Oracle können Sie die Pre- und Post-Task-Skripte für Backup-, Restore- und Klonvorgänge ausführen.

In SnapManager (3.1 oder früher) ist der Abschnitt für die Aufgabenspezifikation Teil der XML-Datei für die Klonspezifikation. Aus SnapManager 3.2 für Oracle ist der Abschnitt „Aufgabenspezifikation“ eine separate XML-Datei.

SnapManager 3.3 oder höher unterstützt nicht die Verwendung der XML-Datei für die Klonspezifikation, die in den Versionen vor SnapManager 3.2 erstellt wurde.

In SnapManager (3.2 oder höher) für Oracle müssen Sie sicherstellen, dass die folgenden Voraussetzungen für einen erfolgreichen SnapManager-Betrieb erfüllt sind:

- Verwenden Sie für Sicherungs- und Wiederherstellungsvorgänge die XML-Datei für die Aufgabenspezifikation.
- Geben Sie für den Klonvorgang zwei Spezifikationsdateien an: Eine XML-Datei für die Klonspezifikation und eine XML-Datei für die Aufgabenspezifikation.

  Wenn Sie Voraufgaben oder Nachaufgaben aktivieren möchten, können Sie optional die XML-Datei für die Aufgabenspezifikation hinzufügen.

Sie können die Aufgabenspezifikationsdatei über die grafische Benutzeroberfläche (GUI) von SnapManager, die Befehlszeilenschnittstelle (CLI) oder einen Texteditor erstellen. Sie müssen eine Erweiterung .XML verwenden, damit die Datei entsprechende Bearbeitungsfunktionen ermöglicht. Vielleicht möchten Sie diese Datei speichern, damit Sie sie für zukünftige Backup-, Restore- und Klonvorgänge verwenden können.

Die XML-Datei für die Aufgabenspezifikation enthält zwei Abschnitte:

- Der Abschnitt „Voraufgaben“ enthält Skripte, die vor Backup-, Wiederherstellungs- und Klonvorgängen ausgeführt werden können.
- Der Abschnitt „Aufgaben nach“ enthält Skripte, die nach Backup-, Restore- und Klonvorgängen ausgeführt werden können.

Die Werte, die in den Abschnitten vor und nach Aufgaben enthalten sind, müssen den folgenden Richtlinien entsprechen:

- Aufgabenname: Der Name der Aufgabe muss mit dem Namen des Skripts übereinstimmen, das bei der Ausführung des Befehls plugin.sh -beschreibe angezeigt wird.

  Wenn eine Diskrepanz besteht, erhalten Sie möglicherweise die folgende Fehlermeldung: Die Datei wurde nicht gefunden.

- Parametername: Der Name des Parameters muss ein String sein, der als Umgebungsvariable-Einstellung verwendet werden kann.

  Die Zeichenfolge muss mit dem Parameternamen im benutzerdefinierten Skript übereinstimmen, das bei der Ausführung des Befehls plugin.sh -beschreibe angezeigt wird.

Sie können die Spezifikationsdatei basierend auf der Struktur der folgenden Beispielaufgabe Spezifikationsdatei erstellen:

```
<task-specification>
  <pre-tasks>
<task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </post-tasks>
</task-specification>
```

Die XML-Datei für die Aufgabenspezifikation darf keine Richtlinien enthalten.

Über die SnapManager-Benutzeroberfläche können Sie den Parameterwert festlegen und die XML-Datei speichern. Sie können die Seite „Task Enabling“ des Assistenten „Backup Create“, „Restore“ oder „Recovery“ und „Clone Create“ verwenden, um die vorhandene XML-Datei für die Aufgabenspezifikation zu laden und die ausgewählte Datei für die Voraufgabe oder die Nachbearbeitung zu verwenden.

Eine Aufgabe kann mehrfach ausgeführt werden, entweder mit den gleichen oder mit unterschiedlichen Parameter- und Wertkombinationen. Zum Beispiel können Sie eine Aufgabe Speichern verwenden, um mehrere Dateien zu speichern.

SnapManager verwendet die in der Aufgabenspezifikationsdatei angegebenen XML-Tags für die Vorverarbeitung oder Nachbearbeitung der Backup-, Wiederherstellungs- und Klonvorgänge unabhängig von der Dateierweiterung der Aufgabenspezifikationsdatei.

Erstellen von vor-, Post-Task- und Richtlinienskripten

SnapManager ermöglicht das Erstellen von Skripten für die Vorverarbeitung, die Nachbearbeitung und die Richtlinienaufgaben für Backup, Wiederherstellung und Klonvorgänge. Sie müssen die Skripte in das richtige Installationsverzeichnis platzieren, um die Vorverarbeitung, die Nachbearbeitungsaktivität und die Richtlinienaufgaben des SnapManager-Vorgangs auszuführen.

Skriptinhalt vor und nach der Aufgabe

Alle Skripte müssen Folgendes enthalten:

- Spezifische Vorgänge (prüfen, beschreiben und ausführen)
- (Optional) vordefinierte Umgebungsvariablen
- Spezifischer Fehlercode (Rückgabecode (rc))

Sie müssen den korrekten Code für die Fehlerbehandlung angeben, um das Skript zu validieren.

Sie können die Vortaskskripte für viele Zwecke verwenden, zum Beispiel, um einen Festplattenspeicher vor dem Start des SnapManager-Vorgangs zu bereinigen. So können Sie beispielsweise auch die Skripts für die Nachbearbeitung verwenden, um einschätzen zu können, ob SnapManager über genügend Festplattenspeicher verfügt, um den Vorgang abzuschließen.

Policy Task Skript Inhalt

Sie können das Richtlinienskript ausführen, ohne bestimmte Aufgaben wie das Prüfen, Beschreiben und Ausführen von auszuführen. Das Skript enthält die vordefinierten Umgebungsvariablen (optional) und den spezifischen Code zur Fehlerbehandlung.

Das Richtlinienskript wird vor der Backup-, Wiederherstellungs- und Klonvorgänge ausgeführt.

- Unterstützte Formate*

Als Prescript und Post-Script kann eine Shell-Script-Datei mit .sh-Erweiterung verwendet werden.

Skript-Installationsverzeichnis

Das Verzeichnis, in dem Sie das Skript installieren, beeinflusst die Verwendung. Sie können die Skripte in das

Verzeichnis platzieren und das Skript ausführen, bevor oder nach dem Backup-, Wiederherstellungs- oder Klonvorgang erfolgt. Sie müssen das Skript in das in der Tabelle angegebene Verzeichnis legen und es auf optionaler Basis verwenden, wenn Sie den Backup-, Wiederherstellungs- oder Klonvorgang angeben.

Sie müssen sicherstellen, dass das Plugin-Verzeichnis die ausführbare Berechtigung hat, bevor Sie die Skripte für den SnapManager-Betrieb verwenden.

Aktivität	Backup	Wiederherstellen	Klon
Vorverarbeitung	<default_Installation_Directory>/Plugins/Backup/create/pre	<default_Installation_Directory>/Plugins/restore/create/pre	<default_Installation_Directory>/Plugins/Clone/create/pre
Nachbearbeitet	<default_Installation_Directory>/Plugins/Backup/create/post	<default_Installation_Directory>/Plugins/restore/create/post	<default_Installation_Directory>/Plugins/Clone/create/post
Richtlinienbasiert	<default_Installation_Directory>/Plugins/Backup/create/Policy	<default_Installation_Directory>/Plugins/restore/create/Policy	<default_Installation_Directory>/Plugins/Clone/create/Policy

Sample scripts Position

Im Folgenden sind einige Beispiele für die Skripte vor und nach der Aufgabe für die Backup- und Klonvorgänge aufgeführt, die im Installationspfad verfügbar sind:

- <default_Installation_Directory>/Plugins/examples/Backup/create/pre
- <default_Installation_Directory>/Plugins/examples/Backup/create/post
- <default_Installation_Directory>/Plugins/examples/Clone/create/pre
- <default_Installation_Directory>/Plugins/examples/Clone/create/post

Was Sie im Skript ändern können

Wenn Sie ein neues Skript erstellen, können Sie nur die Operationen beschreiben und ausführen ändern. Jedes Skript muss die folgenden Variablen enthalten: Kontext, Timeout und Parameter.

Die Variablen, die Sie in der Beschreiben-Funktion des Skripts beschrieben haben, müssen zu Beginn des Skripts deklariert werden. Sie können neue Parameterwerte in Parameter=() hinzufügen und dann die Parameter in der Funktion Ausführen verwenden.

Beispielskript

Im Folgenden ist ein Beispielskript mit einem vom Benutzer angegebenen Rückgabecode zur Schätzung des Speicherplatzes im SnapManager-Host:

```
    #!/bin/bash
    # $Id:
//depot/prod/capstan/main/src/plugins/unix/examples/backup/create/pre/disk
_space_estimate.sh#5 $
```

```
    name="disk space estimation ($(basename $0))"
    description="pre tasks for estimating the space on the target system"
    context=
    timeout="0"
    parameter=()
    EXIT=0
    PRESERVE_DIR="/tmp/preserve/$(date +%Y%m%d%H%M%S)"
    function _exit {
       rc=$1
       echo "Command complete."
       exit $rc
    }
    function usage {
       echo "usage: $(basename $0) { -check | -describe | -execute }"
       _exit 99
    }
    function describe {
       echo "SM_PI_NAME:$name"
       echo "SM_PI_DESCRIPTION:$description"
       echo "SM_PI_CONTEXT:$context"
       echo "SM_PI_TIMEOUT:$timeout"
       IFS=^
       for entry in ${parameter[@]}; do
           echo "SM_PI_PARAMETER:$entry"
       done
       _exit 0
    }
    function check {
       _exit 0
    }
    function execute {
       echo "estimating the space on the target system"
       # Shell script to monitor or watch the disk space
       # It will display alert message, if the (free available) percentage
       # of space is >= 90%
       #
-------------------------------------------------------------------------
       # Linux shell script to watch disk space (should work on other UNIX
oses )
       # set alert level 90% is default
       ALERT=90
       df -H | grep -vE '^Filesystem|tmpfs|cdrom' | awk '{ print $5 " " $1
}' | while read output;
       do
         #echo $output
         usep=$(echo $output | awk '{ print $1}' | cut -d'%' -f1  )
```

```
          partition=$(echo $output | awk '{ print $2 }' )
       if [ $usep -ge $ALERT ]; then
           echo "Running out of space \"$partition ($usep%)\" on
$(hostname) as on $(date)" |
       fi
       done
      _exit 0
     }
    function preserve {
        [ $# -ne 2 ] && return 1
        file=$1
        save=$(echo ${2:0:1} | tr [a-z] [A-Z])
        [ "$save" == "Y" ] || return 0
        if [ ! -d "$PRESERVE_DIR" ] ; then
           mkdir -p "$PRESERVE_DIR"
           if [ $? -ne 0 ] ; then
               echo "could not create directory [$PRESERVE_DIR]"
               return 1
           fi
        fi
        if [ -e "$file" ] ; then
            mv "$file" "$PRESERVE_DIR/."
        fi
        return $?
    }
    case $(echo $1 | tr [A-Z] [a-z]) in
        -check)    check
                  ;;
        -execute)  execute
                  ;;
        -describe) describe
                  ;;
     *)          echo "unknown option $1"
                usage
                ;;
     esac
```

Vorgänge in Taskskripten

Die von Ihnen erstellten Pre-Task- oder Post-Task-Skripte müssen einer Standard-Plug-in-Struktur von SnapManager für Oracle entsprechen.

Die vor- und Nachaufgaben-Skripte müssen die folgenden Vorgänge umfassen:

- Prüfen
- Beschreiben

- Ausführen

Wenn einer dieser Vorgänge nicht im Skript für die Aufgabe vor oder nach der Aufgabe angegeben ist, wird das Skript ungültig.

Wenn Sie den smo Plugin Check Befehl für die Pre-Task oder Post-Task-Skripte ausführen, zeigt der zurückgegebene Status der Skripte Fehler an (da der zurückgegebene Statuswert nicht Null ist).

Betrieb	Beschreibung
Prüfen	Der SnapManager-Server führt den Befehl plugin.sh -Check aus, um sicherzustellen, dass das System über die Ausführungsberechtigung auf den Plug-in-Skripten verfügt. Sie können auch die Überprüfung der Dateiberechtigungen auf dem Remote-System einschließen.

Betrieb	Beschreibung

Beschreiben	Auf dem SnapManager-Server wird der Befehl plugin.sh -beschreibe ausgeführt, um Informationen über Ihr Skript abzurufen und die von der Spezifikationsdatei bereitgestellten Elemente zu entsprechen. Ihr Plug-in-Skript muss die folgenden Beschreibungen enthalten:
	• SM_PI_NAME: Skriptname. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_DESCRIPTION: Beschreibung des Zwecks des Skripts. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_CONTEXT: Kontext, in dem das Skript ausgeführt werden soll, zum Beispiel root oder oracle. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_TIMEOUT: Die maximale Zeit (in Millisekunden), die SnapManager warten sollte, bis das Skript die Verarbeitung beendet und die Ausführung beendet. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_PARAMETER: Ein oder mehrere benutzerdefinierte Parameter, die für die Verarbeitung Ihres Plug-in-Skripts erforderlich sind. Jeder Parameter sollte in einer neuen Ausgabezeile aufgeführt werden und den Namen des Parameters sowie eine Beschreibung enthalten. Wenn das Skript die Verarbeitung abgeschlossen hat, wird Ihrem Skript der Parameterwert durch eine Umgebungsvariable zur Verfügung gestellt.
	Im Folgenden finden Sie eine Beispielausgabe des Skripts Followup_Aktivitäten.
	`plugin.sh - describe`
	`SM_PI_NAME:Followup_activities`
	`SM_PI_DESCRIPTION:this script contains follow-up activities to be executed after the clone create operation.`
	`SM_PI_CONTEXT:root`
	`SM_PI_TIMEOUT:60000`
	`SM_PI_PARAMETER:SCHEMAOWNER:Name of the database schema owner.`
	`Command complete.`

Betrieb	Beschreibung
Ausführen	Der SnapManager-Server führt den Befehl plugin.sh -execute aus, um Ihr Skript zur Ausführung des Skripts zu starten.

Verwandte Informationen

Der smo Plugin Check Befehl

Variablen, die in den Taskskripten für den Backup-Vorgang verfügbar sind

SnapManager stellt Kontextinformationen in Form von Umgebungsvariablen für den durchzuführenden Backup-Vorgang zur Verfügung. Ihr Skript kann beispielsweise den Namen des ursprünglichen Hosts, den Namen der Aufbewahrungsrichtlinie und das Etikett des Backups abrufen.

In der folgenden Tabelle sind die Umgebungsvariablen aufgeführt, die Sie in Ihren Skripten verwenden können:

Variablen	Beschreibung	Formatieren
SM_OPERATION_ID	Gibt die ID des aktuellen Vorgangs an	Zeichenfolge
SM_PROFILE_NAME	Gibt den Namen des verwendeten Profils an	Zeichenfolge
SM_SID	Gibt die Systemkennung der Datenbank an	Zeichenfolge
SM_HOST	Gibt den Hostnamen der Datenbank an	Zeichenfolge
SM_OS_USER	Gibt den Betriebssystemeigentümer der Datenbank an	Zeichenfolge
SM_OS_GROUP	Gibt die Betriebssystemgruppe der Datenbank an	Zeichenfolge
SM_BACKUP_TYP	Gibt den Typ des Backups an (online, offline oder Auto)	Zeichenfolge
SM_BACKUP_LABEL	Gibt die Bezeichnung des Backups an	Zeichenfolge
SM_BACKUP_ID	Gibt die ID des Backups an	Zeichenfolge

Variablen	Beschreibung	Formatieren
SM_BACKUP_RETENTION	Gibt den Aufbewahrungszeitraum an	Zeichenfolge
SM_BACKUP_PROFIL	Gibt das Profil an, das für dieses Backup verwendet wird	Zeichenfolge
SM_ALLOW_DATABASE_SHUTDOWN	Gibt an, ob Sie die Datenbank starten oder herunterfahren möchten Wenn erforderlich, können Sie die Option -Force über die Befehlszeilenschnittstelle verwenden.	boolesch
SM_BACKUP_UMFANG	Gibt den Umfang des Backups an (vollständig oder teilweise)	Zeichenfolge
SM_BACKUP_SCHUTZ	Gibt an, ob der Sicherungsschutz aktiviert ist	boolesch
SM_TARGET_FILER_NAME	Gibt den Namen des Zielspeichersystems an **Hinweis:** Wenn mehr als ein Speichersystem verwendet wird, müssen die Namen des Speichersystems durch Kommas getrennt werden.	Zeichenfolge
SM_TARGET_VOLUME_NAME	Gibt den Namen des Zielvolume an **Hinweis:** der Name des Zielvolumes muss mit dem Namen des Speichergeräts vorbestimmt sein, zum Beispiel SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	Zeichenfolge
SM_HOST_FILE_SYSTEM	Gibt das Host-Dateisystem an	Zeichenfolge
SM_SNAPSHOT_NAMEN	Gibt die Snapshot-Liste an **Hinweis:** der Name der Snapshot-Kopien muss mit dem Namen des Storage-Systems und dem Volume-Namen vorangestellt sein. Die Namen der Snapshot Kopien werden durch Kommata getrennt.	String-Array
SM_ASM_DISK_GROUPS	Gibt die Liste der ASM-Festplattengruppen an	String-Array

Variablen	Beschreibung	Formatieren
SM_ARCHIVE_LOGS_DIRECTORY	Gibt das Verzeichnis der Archivprotokolle an **Hinweis:** Wenn sich die Archivprotokolle in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_REDO_LOGS_DIRECTORY	Gibt das Verzeichnis der Redo-Logs an **Hinweis:** Wenn sich die Redo-Logs in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_CONTROL_FILES_DIRECTORY	Gibt das Verzeichnis der Steuerdateien an **Hinweis:** Wenn sich die Steuerdateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_DATA_FILES_DIRECTORY	Gibt das Verzeichnis der Datendateien an **Hinweis:** Wenn sich die Datendateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
Benutzerdefiniert	Gibt zusätzliche Parameter an, die vom Benutzer definiert werden. Benutzerdefinierte Parameter sind für Plug-ins, die als Richtlinien verwendet werden, nicht verfügbar.	Benutzerdefiniert

Variablen, die in den Taskskripten für den Wiederherstellungsvorgang verfügbar sind

SnapManager stellt Kontextinformationen in Form von Umgebungsvariablen für den durchgeführten Wiederherstellungsvorgang bereit. Ihr Skript kann beispielsweise den Namen des ursprünglichen Hosts und die Bezeichnung des wiederhergestellten Backups abrufen.

In der folgenden Tabelle sind die Umgebungsvariablen aufgeführt, die Sie in Ihren Skripten verwenden können:

Variablen	Beschreibung	Formatieren
SM_OPERATION_ID	Gibt die ID des aktuellen Vorgangs an	Zeichenfolge
SM_PROFILE_NAME	Gibt den Namen des verwendeten Profils an	Zeichenfolge
SM_HOST	Gibt den Hostnamen der Datenbank an	Zeichenfolge
SM_OS_USER	Gibt den Betriebssystemeigentümer der Datenbank an	Zeichenfolge
SM_OS_GROUP	Gibt die Betriebssystemgruppe der Datenbank an	Zeichenfolge
SM_BACKUP_TYP	Gibt den Typ des Backups an (online, offline oder Auto)	Zeichenfolge
SM_BACKUP_LABEL	Gibt die Sicherungsbezeichnung an	Zeichenfolge
SM_BACKUP_ID	Gibt die Backup-ID an	Zeichenfolge
SM_BACKUP_PROFIL	Gibt das Profil an, das für die Sicherung verwendet wird	Zeichenfolge
SM_RECOVERY_TYPE	Gibt die Informationen zur Wiederherstellungskonfiguration an	Zeichenfolge
SM_VOLUME_RESTORE_MODE	Gibt die Wiederherstellungskonfiguration des Volumes an	Zeichenfolge
SM_TARGET_FILER_NAME	Gibt den Namen des Zielspeichersystems an **Hinweis:** Wenn mehr als ein Speichersystem verwendet wird, müssen die Namen des Speichersystems durch Kommas getrennt werden.	Zeichenfolge
SM_TARGET_VOLUME_NAME	Gibt den Namen des Zielvolume an **Hinweis:** der Name des Zielvolumes muss mit dem Namen des Speichergeräts vorbestimmt sein, zum Beispiel SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	Zeichenfolge

Variablen	Beschreibung	Formatieren
SM_HOST_FILE_SYSTEM	Gibt das Host-Dateisystem an	Zeichenfolge
SM_SNAPSHOT_NAMEN	Gibt die Snapshot-Liste an **Hinweis:** der Name der Snapshot-Kopien muss mit dem Namen des Storage-Systems und dem Volume-Namen vorangestellt sein. Die Namen der Snapshot Kopien werden durch Kommata getrennt.	String-Array
SM_ASM_DISK_GROUPS	Gibt die Liste der ASM-Festplattengruppen an	String-Array
SM_ARCHIVE_LOGS_DIRECTORY	Gibt das Verzeichnis der Archivprotokolle an **Hinweis:** Wenn sich die Archivprotokolle in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_REDO_LOGS_DIRECTORY	Gibt das Verzeichnis der Redo-Logs an **Hinweis:** Wenn sich die Redo-Logs in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_CONTROL_FILES_DIRECTORY	Gibt das Verzeichnis der Steuerdateien an **Hinweis:** Wenn sich die Steuerdateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_DATA_FILES_DIRECTORY	Gibt das Verzeichnis der Datendateien an **Hinweis:** Wenn sich die Datendateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array

In den Aufgabenskripten verfügbare Variablen für den Klonvorgang

SnapManager stellt Kontextinformationen in Form von Umgebungsvariablen für den ausgeführten Klonvorgang bereit. Ihr Skript kann beispielsweise den Namen des

ursprünglichen Hosts, den Namen der Klondatenbank und den Namen des Backups abrufen.

In der folgenden Tabelle sind die Umgebungsvariablen aufgeführt, die Sie in Ihren Skripten verwenden können:

Variablen	Beschreibung	Formatieren
SM_ORIGINAL_SID	SID der ursprünglichen Datenbank	Zeichenfolge
SM_URSPRÜNGLICHER_HOST	Der ursprünglichen Datenbank zugeordnete Hostname	Zeichenfolge
SM_ORIGINAL_OS_USER	OS-Eigentümer der ursprünglichen Datenbank	Zeichenfolge
SM_ORIGINAL_OS_GROUP	OS-Gruppe der ursprünglichen Datenbank	Zeichenfolge
SM_TARGET_SID	SID der Klondatenbank	Zeichenfolge
SM_TARGET_HOST	Der Klondatenbank zugeordnete Host-Name	Zeichenfolge
SM_TARGET_OS_USER	OS-Eigentümer der Klondatenbank	Zeichenfolge
SM_TARGET_OS_GROUP	OS-Gruppe der Klondatenbank	Zeichenfolge
SM_TARGET_DB_PORT	Port der Zieldatenbank	Ganzzahl
SM_TARGET_GLOBAL_DB_NAME	Globaler Datenbankname der Zieldatenbank	Zeichenfolge
SM_BACKUP_LABEL	Bezeichnung des für den Klon verwendeten Backups	Zeichenfolge

Fehlerbehandlung in benutzerdefinierten Skripts

SnapManager verarbeitet das benutzerdefinierte Skript auf Basis der jeweiligen Rückgabecodes. Wenn Ihr benutzerdefiniertes Skript beispielsweise den Wert 0, 1, 2 oder 3 zurückgibt, wird der Klonprozess von SnapManager fortgesetzt. Der Rückgabecode beeinflusst auch die Prozesse von SnapManager und gibt die Standardausgabe Ihrer Skriptausführung zurück.

Rückgabecode	Beschreibung	Fahren Sie mit der Verarbeitung des Vorgangs fort
0	Das Skript wurde erfolgreich abgeschlossen.	Ja.
1	Das Skript wurde erfolgreich mit Informationsmeldungen abgeschlossen.	Ja.
2	Das Skript wurde abgeschlossen, enthält jedoch Warnungen	Ja.
3	Das Skript schlägt fehl, der Vorgang wird jedoch fortgesetzt.	Ja.
4 oder >4	Das Skript schlägt fehl, und der Vorgang wird beendet.	Nein

Anzeigen von Beispielskripten für das Plug-in

SnapManager enthält Skripte, die Sie als Beispiele dafür verwenden können, wie Sie Ihre eigenen Skripte oder als Grundlage für Ihre benutzerdefinierten Skripts erstellen.

Die Beispielskripts für das Plug-in finden Sie unter folgender Adresse:

- <default_install_Directory>/Plugins/examples/Backup/create
- <default_install_Directory>/Plugins/examples/Clone/create
- <default_install_Directory>/Plugins/unix/examples/Backup/create/post

Das Verzeichnis, das die Beispiel-Plug-in-Skripte enthält, umfasst die folgenden Unterverzeichnisse:

- Richtlinie: Enthält Skripte, die, wenn sie konfiguriert sind, immer im Klonvorgang ausgeführt werden.
- Pre: Enthält Skripte, die, wenn konfiguriert, vor dem Klonvorgang ausgeführt werden.
- Post: Enthält Skripte, die, wenn sie konfiguriert sind, nach dem Klonvorgang ausgeführt werden.

Die folgende Tabelle beschreibt die Beispielskripts:

Skriptname	Beschreibung	Skripttyp
validate_sid.sh	Enthält zusätzliche Prüfungen für den auf dem Zielsystem verwendeten SID. Das Skript überprüft, ob der SID die folgenden Eigenschaften hat: • Enthält drei alphanumerische Zeichen • Beginnt mit einem Buchstaben	Richtlinie
cleanup.sh	Reinigt das Zielsystem, so dass es bereit ist, den neu erstellten Klon zu speichern. Speichert oder löscht Dateien und Verzeichnisse je nach Bedarf.	Voraufgabe
Mirror_the_backup.sh	Spiegelung der Volumes nach dem Backup in einer UNIX-Umgebung bei Verwendung von Data ONTAP im 7-Mode oder Clustered Data ONTAP	Aufgabe einstellen
Vault_the_backup_cDOT.sh	Vaults das Backup, nachdem der Backup-Vorgang in einer UNIX-Umgebung ausgeführt wurde, wenn Sie Clustered Data ONTAP verwenden.	Aufgabe einstellen

Mit SnapManager gelieferte Skripte verwenden standardmäßig die BASH Shell. Sie müssen sicherstellen, dass die Unterstützung für DIE BASH-Shell auf Ihrem Betriebssystem installiert ist, bevor Sie versuchen, einen der Beispielskripte auszuführen.

1. Um zu überprüfen, ob Sie die BASH-Shell verwenden, geben Sie den folgenden Befehl an der Eingabeaufforderung ein: `bash`

   Wenn kein Fehler auftritt, funktioniert DIE BASH-Shell ordnungsgemäß.

   Sie können alternativ den Befehl which-bash an der Eingabeaufforderung eingeben.

2. Suchen Sie das Skript im folgenden Verzeichnis:

   <installdir>/Plugins/Beispiele/Clone/create

3. Öffnen Sie das Skript in einem Skript-Editor wie vi.

Beispielskript

Das folgende benutzerdefinierte Beispielskript validiert die Namen der Datenbank-SID und verhindert, dass ungültige Namen in der geklonten Datenbank verwendet werden. Es umfasst drei Operationen (prüfen, beschreiben und ausführen), die aufgerufen werden, nachdem Sie das Skript ausgeführt haben. Das Skript

enthält auch Fehlermeldungs-Handling mit den Codes 0, 4 und >4.

```
EXIT=0
name="Validate SID"
description="Validate SID used on the target system"
parameter=()

# reserved system IDs
INVALID_SIDS=("ADD" "ALL" "AND" "ANY" "ASC"
              "COM" "DBA" "END" "EPS" "FOR"
              "GID" "IBM" "INT" "KEY" "LOG"
              "MON" "NIX" "NOT" "OFF" "OMS"
              "RAW" "ROW" "SAP" "SET" "SGA"
              "SHG" "SID" "SQL" "SYS" "TMP"
              "UID" "USR" "VAR")
function _exit {
     rc=$1
     echo "Command complete."
        return $rc}

function usage {
     echo "usage: $(basename $0) { -check | -describe | -execute }"
     _exit 99}

function describe {
        echo "SM_PI_NAME:$name"
        echo "SM_PI_DESCRIPTION:$description"
        _exit 0}

function check {
        _exit 0}

function execute {
        IFS=\$ myEnv=$(env)
     for a in ${paramteter[@]}; do
            key=$(echo ${$a} | awk -F':' '{ print $1 }')
         val=$(echo $myEnv | grep -i -w $key 2>/dev/null | awk -F'=' '{
print $2 }')

            if [ -n "$val" ] ; then
              state="set to $val"
            else
                    state="not set"
                    #indicate a FATAL error, do not continue processing
                    ((EXIT=+4))
               fi
```

```
          echo "parameter $key is $state"
     done

    ########################################################################
    # additional checks
 # Use SnapManager environment variable of SM_TARGET_SID

    if [ -n "$SM_TARGET_SID" ] ; then
        if [ ${#SM_TARGET_SID} -ne 3 ] ; then
        echo "SID is defined as a 3 digit value, [$SM_TARGET_SID] is not
valid."
        EXIT=4
    else
        echo "${INVALID_SIDS[@]}" | grep -i -w $SM_TARGET_SID >/dev/null
2>&1
                if [ $? -eq 0 ] ; then
            echo "The usage of SID [$SM_TARGET_SID] is not supported by
SAP."
                        ((EXIT+=4))
        fi
    fi
    else
        echo "SM_TARGET_SID not set"
     EXIT=4
    fi  _exit $EXIT}

# Include the 3 required operations for clone plugin
case $(echo "$1" | tr [A-Z] [a-z]) in
  -check )        check     ;;
  -describe )     describe  ;;
  -execute )      execute   ;;      * )
         echo "unknown option $1"    usage      ;;
esac
```

Aufgabenskripte werden erstellt

Sie können die Task-Skripte für vor- und Nachaufgaben sowie Richtlinien für Backup-, Restore- und Klonvorgänge erstellen, das Skript schreiben und die vordefinierten Umgebungsvariablen in Ihren Parametern einbeziehen. Sie können entweder ein neues Skript erstellen oder eines der SnapManager Beispielskripte ändern.

Bevor Sie mit dem Erstellen des Skripts beginnen, stellen Sie sicher, dass:

- Sie müssen das Skript auf eine bestimmte Weise strukturieren, damit es im Kontext einer SnapManager-Operation ausgeführt werden kann.
- Sie müssen das Skript auf der Grundlage der erwarteten Vorgänge, der verfügbaren Eingabeparameter

und der Rückgabekonventionen erstellen.

- Sie müssen Protokollmeldungen einschließen und die Meldungen zu benutzerdefinierten Protokolldateien umleiten.

  a. Erstellen Sie das Aufgabenskript, indem Sie das Beispielskript anpassen.

     Führen Sie Folgendes aus:

     i. Suchen Sie ein Beispielskript im folgenden Installationsverzeichnis:

        <default_install_Directory>/Plugins/examples/Backup/create

     <default_install_Directory>/Plugins/examples/Clone/create

     i. Öffnen Sie das Skript in Ihrem Skript-Editor.
     ii. Speichern Sie das Skript mit einem anderen Namen.

  b. Ändern Sie die Funktionen, Variablen und Parameter nach Bedarf.

  c. Das Skript in einem der folgenden Verzeichnisse speichern:

     Skripts für Backup-Vorgänge

     - <default_install_Directory>/Plugins/Backup/create/pre: Führt das Skript aus, bevor der Backup-Vorgang durchgeführt wird. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
     - <default_install_Directory>/Plugins/Backup/create/post: Führt das Skript nach dem Backup-Vorgang aus. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
     - <default_install_Directory>/Plugins/Backup/create/Policy: Führt das Skript immer aus, bevor der Backup-Vorgang stattfindet. SnapManager verwendet dieses Skript immer für alle Backups im Repository. **Betriebsskripte wiederherstellen**
     - <default_install_Directory>/Plugins/restore/create/pre: Führt das Skript aus, bevor der Backup-Vorgang durchgeführt wird. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
     - <default_install_Directory>/Plugins/restore/create/post: Führt das Skript nach dem Backup-Vorgang aus. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
     - <default_install_Directory>/Plugins/restore/create/Policy: Führt das Skript immer aus, bevor der Backup-Vorgang stattfindet. SnapManager verwendet dieses Skript immer für alle Backups im Repository. **Clone Operation Scripts**
     - <default_install_Directory>/Plugins/Clone/create/pre: Führt das Skript aus, bevor der Backup-Vorgang durchgeführt wird. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
     - <default_install_Directory>/Plugins/Clone/create/post: Führt das Skript nach dem Backup-Vorgang aus. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
     - <default_install_Directory>/Plugins/Clone/create/Policy: Führt das Skript immer aus, bevor der Backup-Vorgang erfolgt. SnapManager verwendet dieses Skript immer für alle Backups im Repository.

Speichern der Taskskripte

Sie müssen die Skript für Aufgaben vor, nach und nach der Aufgabe sowie die Richtlinien in einem bestimmten Verzeichnis auf dem Zielserver speichern, auf dem die Backups oder Klone erstellt werden. Für den Wiederherstellungsvorgang müssen die Skripte in das angegebene Verzeichnis auf dem Zielserver platziert werden, auf dem Sie das

Backup wiederherstellen möchten.

1. Erstellen Sie Ihr Skript.
2. Speichern Sie das Skript an einem der folgenden Speicherorte:

Für den Backup-Vorgang

Verzeichnis	Beschreibung
<default_install_Directory >/Plugins/Backup/create/Policy	Die Richtlinieskripte werden vor den Backup-Vorgängen ausgeführt.
<default_install_Directory >/Plugins/Backup/create/pre	Die Vorverarbeitungsskripte führen die vor dem Backup aus.
<default_install_Directory >/Plugins/Backup/create/post	Die nachverarbeitenden Skripte werden nach den Backup-Vorgängen ausgeführt.

Für den Wiederherstellungsvorgang

Verzeichnis	Beschreibung
<default_install_Directory >/Plugins/restore/create/Policy	Die Richtlinienskripte werden vor den Wiederherstellungsvorgängen ausgeführt.
<default_install_Directory >/Plugins/restore/create/pre	Die Vorverarbeitungsskripte werden vor der Wiederherstellung ausgeführt.
<default_install_Directory >/Plugins/restore/create/post	Die nachverarbeitenden Skripte werden nach den Wiederherstellungsvorgängen ausgeführt.

Für den Klonvorgang

Verzeichnis	Beschreibung
<default_install_Directory >/Plugins/Clone/create/Policy	Die Richtlinisskripte werden vor dem Klonbetrieb ausgeführt.
<default_install_Directory >/Plugins/Clone/create/pre	Die Vorverarbeitungsskripte werden vor den Klonvorgängen ausgeführt.
<default_install_Directory >/Plugins/Clone/create/post	Die nachverarbeitenden Skripte werden nach den Klonvorgängen ausgeführt.

Überprüfen der Installation von Plug-in-Skripten

SnapManager ermöglicht Ihnen die Installation und Verwendung benutzerdefinierter Skripte zur Ausführung verschiedener Vorgänge. SnapManager bietet Plug-ins für

Backup-, Restore- und Klonvorgänge, mit denen Sie Ihre benutzerdefinierten Skripts vor und nach dem Backup-, Restore- und Klonvorgängen automatisieren können.

1. Geben Sie den folgenden Befehl ein:

   bbs Plugin Check -osccount os db Benutzername

   Wenn Sie die Option -osconger nicht bereitstellen, erfolgt die Überprüfung der Plug-in-Script-Installation für den Root-Benutzer statt für einen bestimmten Benutzer.

   Der folgende Ausgang zeigt an, dass die Skripte „Policy 1“, „pre-Plugin1“ und „pre-Plugin2“ erfolgreich installiert wurden. Das Post-Plugin1-Skript ist jedoch nicht funktionsfähig.

```
            smo plugin check
Checking plugin directory structure ...
<installdir>/plugins/clone/policy
   OK: 'policy1' is executable

<installdir>/plugins/clone/pre
   OK: 'pre-plugin1' is executable and returned status 0
   OK: 'pre-plugin2' is executable and returned status 0

<installdir>/plugins/clone/post
   ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

Erstellen einer Aufgabenspezifikationsdatei

Sie können die Aufgabenspezifikationsdateien über eine grafische Benutzeroberfläche (GUI), eine Befehlszeilenschnittstelle (CLI) oder einen Texteditor erstellen. Diese Dateien werden für die vor- oder Nachverarbeitung während der Backup-, Restore- und Klonvorgänge verwendet.

1. Erstellen Sie eine Aufgabenspezifikationsdatei über GUI, CLI oder einen Texteditor.

   Sie können die Spezifikationsdatei basierend auf der Struktur der folgenden Beispielaufgabe Spezifikationsdatei erstellen:

```
<task-specification>
  <pre-tasks>
                <task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </post-tasks>
</task-specification>
```

2. Geben Sie den Skriptnamen ein.
3. Geben Sie den Parameternamen und den dem Parameter zugewiesenen Wert ein.
4. Speichern Sie die XML-Datei im richtigen Installationsverzeichnis.

Beispiel für Aufgabenspezifikation

```
  <task-specification>
    <pre-tasks>
      <task>
        <name>clone cleanup</name>
        <description>pre tasks for cleaning up the target
system</description>
        </task>
    </pre-tasks>
    <post-tasks>
      <task>
        <name>SystemCopy follow-up activities</name>
        <description>SystemCopy follow-up activities</description>
        <parameter>
          <name>SCHEMAOWNER</name>
          <value>SAMSR3</value>
        </parameter>
      </task>
      <task>
        <name>Oracle Users for OS based DB authentication</name>
        <description>Oracle Users for OS based DB
authentication</description>
        <parameter>
          <name>SCHEMAOWNER</name>
          <value>SAMSR3</value>
        </parameter>
        <parameter>
          <name>ORADBUSR_FILE</name>

<value\>/mnt/sam/oradbusr.sql</value\>

        </parameter>
      </task>
      </post-tasks>
  </task-specification>
```

Durchführung von Backup-, Restore- und Klonvorgängen mithilfe von Prescript und Post-Scripts

Sie können Ihr eigenes Skript verwenden, während Sie Backup-, Restore- oder Klonvorgang initiieren. SnapManager zeigt eine Seite für die Aktivierung von Aufgaben im Assistenten zum Erstellen von Backups, zum Wiederherstellen oder Wiederherstellen oder zum Erstellen von Klonen an, wo Sie das Skript auswählen und Werte für alle Parameter angeben können, die vom Skript benötigt werden.

- Installieren Sie die Plug-in-Skripte am richtigen Speicherort für die SnapManager-Installation.

- Überprüfen Sie, ob die Plug-ins korrekt installiert sind, indem Sie den Befehl smo Plugin Check verwenden.
- Stellen Sie sicher, dass Sie die BASH-Shell verwenden.

Führen Sie in der Befehlszeilenschnittstelle (CLI) den Skriptnamen auf, wählen Sie die Parameter aus und legen Sie die Werte fest.

1. Um zu überprüfen, ob Sie die BASH-Shell verwenden, geben Sie den folgenden Befehl an der Eingabeaufforderung:bash ein

   Alternativ können Sie an der Eingabeaufforderung den Befehl which-bash eingeben und die Befehlsausgabe als Startparameter des Skripts verwenden.

   Die BASH-Shell funktioniert einwandfrei, wenn kein Fehler auftritt.

2. Geben Sie für den Backup-Vorgang die Option -taskSpec ein und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation ein, um eine Vorverarbeitung oder eine Nachbearbeitung durchzuführen, die vor oder nach dem Backup durchgeführt werden soll: bbs Backup create -profile_Name {[-full {-online { -offline} [-contake {-hourly [-Daily { -Weekly} -unlimited}] [-confirm] [-dataces [-monthly-commentaces [-monthly-contaces] [-monthly-commoceptaces [-monthly}] [-monthly-commoceptaces [-monthly] [-monthly-loceptaces] [-] [-monthly-monthly] [-monthly-loceptaces [-] [-monthly-lo [-protect}} -notnow] [-Backup-destpath1 [,[path2]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all - untilSCN -vor {}-dateyyyy-MM-dd HH:mm:ss [-estune-Backups] [-estune-prune-Backups]

   Wenn der Backup-Plug-in-Vorgang fehlgeschlagen ist, werden nur der Plug-in-Name und der Rückgabecode angezeigt. Ihr Plug-in-Skript muss Protokollmeldungen enthalten und die Meldungen an die benutzerdefinierten Protokolldateien weiterleiten.

3. Für den Backup-Restore-Vorgang: Geben Sie die Option -taskspecs ein und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation an, um vor oder nach der Wiederherstellung eine Vorverarbeitung oder eine Nachbearbeitung durchzuführen:Smo Backup Restore -profilprofile_Name {-Label<Label> -id<id>} {-files<<tablespec<tablespaces}> -complete / -controlfiles} [-recover {←alllogs -nologs] -From-secondary [-temp-Volume <temp_Volume>] [-copy-idid]][-taskspec<tassspec>] [-verify][-Force] Backup restore -fast [requited [-rejed] [-dump [-quiet [-verbose]

   Wenn der Vorgang zum Wiederherstellen des Plug-ins fehlgeschlagen ist, werden nur der Plug-in-Name und der Rückgabecode angezeigt. Ihr Plug-in-Skript muss Protokollmeldungen enthalten und die Meldungen an die benutzerdefinierten Protokolldateien weiterleiten.

4. Geben Sie für den Vorgang „Clone create“ die Option -taskSpec ein und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation ein, um eine Vorverarbeitung oder eine Nachbearbeitung durchzuführen, die vor oder nach dem Klonvorgang stattfinden soll: bbs Clone create -profilprofile_Name {-Backup-labelBackup_Name←Backup-id} Backup-id> -current←newsidneft_sid -clonespepfull_path_to_clonespepfile [-Reserve<yes, no, erben>] [-Host<>] [-Label<Label>] [-comment<{<comment> dump [-von-sekundäre [-copy-bose-id]

   Wenn der Klon-Plug-in-Vorgang fehlgeschlagen ist, werden nur der Plug-in-Name und der Rückgabecode angezeigt. Ihr Plug-in-Skript muss Protokollmeldungen enthalten und die Meldungen an die benutzerdefinierten Protokolldateien weiterleiten.

Beispiel für die Erstellung eines Backups mithilfe der XML-Datei für die Aufgabenspezifikation

```
smo backup create -profile SALES1 -full -online -taskspec
sales1_taskspec.xml -force -verify
```

Der Name des Speichersystems und der dem Profil zugeordneten Zieldatenbank-Hostname werden aktualisiert

Mit SnapManager 3.3 oder höher können Sie den Host-Namen des Speichersystems oder die Speichersystemadresse und den dem SnapManager-Profil zugeordneten Host-Namen der Zieldatenbank aktualisieren.

Der Name des Speichersystems, der einem Profil zugeordnet ist, wird aktualisiert

Mit SnapManager 3.3 oder höher können der Hostname oder die IP-Adresse eines Speichersystems, das einem Profil zugeordnet ist, aktualisiert werden.

Sie müssen Folgendes sicherstellen:

- Das Profil verfügt über mindestens eine Sicherung.

  Wenn das Profil keine Sicherungskopie hat, ist es nicht erforderlich, den Namen des Speichersystems für dieses Profil zu aktualisieren.

- Für das Profil wird kein Vorgang ausgeführt.

Sie können den Namen des Storage-Systems oder die IP-Adresse über die SnapManager Befehlszeilenschnittstelle (CLI) aktualisieren. Beim Aktualisieren des Namens des Speichersystems werden die in der Repository-Datenbank gespeicherten Metadaten aktualisiert. Nachdem Sie den Namen des Storage-Systems umbenannt haben, können Sie alle SnapManager-Vorgänge wie zuvor ausführen.

Sie können den Namen des Storage-Systems nicht mit der SnapManager Graphical User Interface (GUI) ändern.

Sie müssen sicherstellen, dass Snapshot Kopien im neuen Storage-System verfügbar sind. SnapManager überprüft nicht, ob die Snapshot Kopien im Storage-System vorhanden sind.

Sie müssen jedoch Folgendes beachten, während Sie ein Rolling Upgrade und Rollback des Hosts durchführen, nachdem Sie den Namen des Speichersystems umbenannt haben:

- Wenn Sie nach der Umbenennung des Speichersystemnamens ein Rolling Upgrade des Hosts durchführen, müssen Sie das Profil mit dem neuen Speichersystemnamen aktualisieren.

  Informationen zur Verwendung der SnapDrive-Befehle zum Ändern des Speichersystemnamens finden Sie unter *Fehlerbehebung bei Problemen mit dem Speichersystemnamen*.

- Wenn Sie den Host nach der Umbenennung des Storage-Systems wieder starten, müssen Sie sicherstellen, dass Sie den Namen des Storage-Systems zurück auf den früheren Namen des Storage-Systems ändern, damit Sie die Profile, Backups und Klone des früheren Storage-Systems zur Durchführung von SnapManager-Vorgängen verwenden können.

Wenn SnapDrive das Speichersystem nicht identifizieren konnte und Fehlermeldungen anzeigt, können Sie den Befehl ipmigrate mit den früheren und höheren Hostnamen des Speichersystems eingeben. Weitere Informationen zu Problemen mit dem Speichersystemnamen finden Sie unter *Fehlerbehebung von Problemen mit dem Namen des Speichersystems*.

1. Geben Sie den folgenden Befehl ein: `smo storage rename -profileprofile -oldnameold_storage_name-newnamenew_storage_name [quiet | -verbose]`

Ihr Ziel ist	Dann…
Aktualisieren Sie den Namen des Speichersystems, der einem Profil zugeordnet ist	Geben Sie die Option -profile an.
Aktualisieren Sie den Namen des Speichersystems oder die IP-Adresse, die einem Profil zugeordnet ist	Geben Sie die folgenden Optionen und Variablen an: • -Oldnameold_Storage_Name ist der Hostname oder die IP-Adresse des Speichersystems. • -Newnamenew_Storage_Name ist der Hostname oder die IP-Adresse des Speichersystems.

Im folgenden Beispiel wird der aktualisierte Speichersystemname angezeigt:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Verwandte Informationen

Fehlerbehebung bei der Umbenennung des Speichersystems

Anzeigen einer Liste von Speichersystemen, die einem Profil zugeordnet sind

Sie können eine Liste der Speichersysteme anzeigen, die einem bestimmten Profil zugeordnet sind.

Die Liste zeigt die Namen des Speichersystems an, die dem jeweiligen Profil zugeordnet sind.

Wenn für das Profil keine Backups verfügbar sind, können Sie den dem Profil zugeordneten Namen des Speichersystems nicht anzeigen.

1. Um Informationen zu Storage-Systemen anzuzeigen, die einem bestimmten Profil zugeordnet sind, geben Sie den folgenden Befehl ein: `smo storage list -profileprofile [-quiet | -verbose]`

Beispiel

```
smo storage list -profile mjubllian
```

```
Sample Output:
Storage Controllers
--------------------
STCO1110-RTP07OLD
```

Der Host-Name der Zieldatenbank, der einem Profil zugeordnet ist, wird aktualisiert

SnapManager (3.2 oder höher) für Oracle bietet die Möglichkeit, den Hostnamen der Zieldatenbank im SnapManager-Profil zu aktualisieren.

- Das Home-Verzeichnis des lokalen Benutzers muss die Zuordnung zu den Profilen und Repositorys kennen.
- Die Sitzungen der SnapManager Graphical User Interface (GUI) müssen geschlossen werden.
- In einer RAC-Umgebung (Real Application Clusters) müssen die auf dem im Profil angegebenen Host verfügbaren Klone oder gemounteten Backups gelöscht und abgehängt werden.

Sie können das Profil mit dem neuen Hostnamen aktualisieren, indem Sie nur die CLI verwenden.

Szenarien werden nicht unterstützt, wenn der Hostname der Zieldatenbank im Profil geändert werden soll

Die folgenden Szenarien werden beim Ändern des Hostnamen der Zieldatenbank im Profil nicht unterstützt:

- Ändern des Host-Namens der Zieldatenbank mithilfe der SnapManager-GUI
- Rollback der Repository-Datenbank nach Aktualisierung des Host-Namens der Zieldatenbank des Profils durchführen
- Aktualisieren mehrerer Profile für einen neuen Hostnamen der Zieldatenbank durch Ausführen eines einzigen Befehls
- Ändern des Host-Namens der Zieldatenbank, wenn ein SnapManager-Vorgang ausgeführt wird
- Ändern des Host-Namens der Zieldatenbank, wenn SnapManager auf Solaris installiert ist und wenn die Datenbank-LUNs (Logical Unit Numbers) mithilfe eines Host-gemounteten Dateisystems mit SVM-Stack erstellt werden.

Nachdem Sie den Hostnamen der Zieldatenbank im Profil aktualisiert haben, wird nur der Hostname der Zieldatenbank geändert. Alle anderen Konfigurationsparameter, die im Profil festgelegt sind, werden beibehalten.

Nachdem Sie den Host-Namen der neuen Zieldatenbank in einem geschützten Profil aktualisiert haben, werden für das aktualisierte Profil dieselben Datensatz- und Sicherungsrichtlinien beibehalten.

Nachdem Sie den Hostnamen für den Zielhost geändert haben, müssen Sie sicherstellen, dass Sie den Hostnamen für alle vorhandenen geschützten Profile aktualisieren, bevor Sie die neuen geschützten Profile erstellen. Um den Hostnamen für ein Profil zu aktualisieren, führen Sie den Befehl smo profile Update aus.

Nachdem Sie den Hostnamen der Zieldatenbank aktualisiert haben, können Sie den Klon nicht trennen oder

das Backup unmounten, wenn das Clone oder bereitgestellte Backup nicht auf dem neuen Host verfügbar ist. In solchen Szenarien führen die Ausführung der SnapManager Vorgänge vom neuen Host zu Ausfällen sowie zu veralteten Einträgen im früheren Host. Um SnapManager-Vorgänge durchzuführen, müssen Sie zum früheren Hostnamen mithilfe der Profilaktualisierung zurücksetzen.

1. Geben Sie den folgenden Befehl ein: `smo profile update -profileprofile [-profile-passwordprofile_password][-database-dbnamedb_dbname-hostdb_host [-siddb_sid] [-login-usernamedb_username-passworddb_password-portdb_port]] [{-rman{-controlfile | {-login-usernamerman_username-passwordrman_password-tnsnamerman_tnsname}}} | -remove-rman]-osaccountosaccount-osgrouposgroup [-retain [-hourly [-countn] [-durationm]] [-daily [-countn] [-durationm]] [-weekly [-countn] [-durationm]] [-monthly [-countn] [-durationm]]] [-commentcomment][-snapname-patternpattern][[-protect [-protection-policypolicy_name]]| [[-noprotect]] [-summary-notification] [-notification [-success-emailemail_address1, email_address2-subjectsubject_pattern] [-failure-emailemail_address1, email_address2-subjectsubject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hourshours | -daysdays | -weeksweeks| -monthsmonths [-protect [-protection-policypolicy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]`

   Weitere Optionen für diesen Befehl:

   [-Force] [-noprompt]

Ihr Ziel ist	Dann…
Ändern Sie den Hostnamen der Zieldatenbank	Geben Sie -hostNew_db_Host an

2. Geben Sie den folgenden Befehl ein, um den Host-Namen der Zieldatenbank des Profils anzuzeigen: `smo profile show`

Historie von SnapManager-Vorgängen aufrechterhalten

Mit SnapManager für Oracle können Sie den Verlauf der SnapManager Vorgänge, die mit einem einzelnen Profil oder mehreren Profilen verknüpft sind, beibehalten. Sie können den Verlauf entweder über die SnapManager Befehlszeilenschnittstelle (CLI) oder über die grafische Benutzeroberfläche (GUI) aufrechterhalten. Sie können die Historie der Vorgänge als Bericht anzeigen und den Bericht zu Audit-Compliance-Zwecken verwenden.

Sie können den Verlauf der folgenden SnapManager Vorgänge beibehalten:

- Backup erstellen
- Backup verifizieren
- Backup Restore
- Klon erstellen
- Aufteilung klonen

Die Verlaufsinformationen für die SnapManager Vorgänge werden basierend auf der Aufbewahrung beibehalten. Sie können für jeden der unterstützten SnapManager Vorgänge unterschiedliche Aufbewahrungsklassen konfigurieren.

Im Folgenden sind einige Aufbewahrungsklassen aufgeführt, die Sie zuweisen können:

- Anzahl Tage
- Anzahl Wochen
- Anzahl Monate
- Anzahl an Operationen

Basierend auf der Aufbewahrung bereinigt SnapManager die Historie automatisch. Außerdem können Sie die Historie der SnapManager-Vorgänge manuell löschen. Wenn Sie das Profil löschen oder zerstören, werden alle dem Profil zugeordneten Verlaufsdaten gelöscht.

Nach dem Rollback des Hosts können Sie die Verlaufsdaten nicht anzeigen oder mit dem Profil, das für die Verlaufswartung konfiguriert wurde, verbundene Vorgänge durchführen.

Konfigurieren des Verlaufs für den SnapManager-Vorgang

Mit SnapManager für Oracle können Sie den Verlauf des SnapManager-Betriebs über die Befehlszeilenschnittstelle oder Benutzeroberfläche von SnapManager aufrechterhalten. Sie können den Verlauf der SnapManager-Operation als Bericht anzeigen.

1. Um den Verlauf der SnapManager-Operation zu konfigurieren, geben Sie folgenden Befehl ein: smo history set -profile {-Name, profile_Name [profile_name1, profile_name2] -all-Repository-Login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname_portrepo_Port} -Operation {} {}-operationOperation_Name [unbose_restay_all_restay_restay_rejour]

```
        smo
history set -profile -name PROFILE1 -operation -operations backup -retain
-daily 6 -verbose
```

```
        smo
history set -profile -name PROFILE1 -operation -all -retain -weekly 3
-verbose
```

Anzeigen einer Liste des SnapManager-Betriebsverlaufs

Sie können den Verlauf eines bestimmten oder aller SnapManager Vorgänge basierend auf den Aufbewahrungseinstellungen als Bericht anzeigen.

1. Geben Sie den folgenden Befehl ein, um eine Liste der SnapManager-Verlaufs-Vorgänge anzuzeigen: `smo history list -profile {-name, profile_name [profile_name1,profile_name2] | -all-repository-login [-passwordrepo_password] -usernamerepo_username -dbnamerepo_dbname-hostrepo_host-portrepo_port} -operation {-operationsoperation_name [operation_name1, operation_name2] | -all} [-`

```
delimiterdelimiter] [-quiet | -verbose]
```

Anzeigen des detaillierten Verlaufs einer bestimmten Operation, die einem Profil zugeordnet ist

Sie können den detaillierten Verlauf einer bestimmten SnapManager Operation anzeigen, die einem Profil zugeordnet ist.

1. Um detaillierte Verlaufsinformationen über eine bestimmte SnapManager-Operation anzuzeigen, die einem Profil zugeordnet ist, geben Sie den folgenden Befehl ein: `smo history operation-show -profileprofile_name {-labellabel | -idid} [-quiet | -verbose]`

Löschen des Verlaufs des SnapManager-Vorgangs

Sie können den Verlauf des SnapManager-Vorgangs löschen, wenn Sie keine Verlaufsdetails mehr benötigen.

1. Geben Sie den folgenden Befehl ein, um den Verlauf des SnapManager-Vorgangs zu löschen: `smo history purge -profile {-name, profile_nameprofile_name1, profile_name2] | all-repository-login [-passwordrepo_password] -usernamerepo_username -dbnamerepo_dbname-hostrepo_host-portrepo_port} -operation {-operationsoperation_name [operation_name1, operation_name2] | -all} [-quiet | -verbose]`

Entfernen von Verlaufseinstellungen, die einem einzelnen Profil oder mehreren Profilen zugeordnet sind

Mit SnapManager können Sie die Verlaufseinstellungen eines SnapManager-Vorgangs entfernen. Mit diesem Vorgang werden alle Verlaufsdaten gelöscht, die mit einem einzelnen Profil oder mehreren Profilen verknüpft sind.

1. Um den Verlauf der SnapManager Vorgänge zu entfernen, die mit einem einzelnen Profil oder mehreren Profilen verknüpft sind, geben Sie den folgenden Befehl ein: `smo history remove -profile {-name, profile_name [profile_name1, profile_name2] | all-repository-login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname-hostrepo_host -portrepo_port} -operation {-operationsoperation_name [operation_name1, operation_name2] | -all} [-quiet | -verbose]`

Anzeigen der Konfigurationsdetails des SnapManager-Verlaufs

Sie können die Verlaufseinstellungen für ein einzelnes Profil anzeigen.

Im SnapManager-Verlauf werden für jedes Profil die folgenden Informationen angezeigt:

- Name des Vorgangs
- Aufbewahrungsklasse
- Anzahl der Aufbewahrung
  a. Um Informationen über den Vorgang der SnapManager-Historie für ein bestimmtes Profil anzuzeigen, geben Sie den folgenden Befehl ein: `smo history show -profileprofile_name`

Befehlsreferenz für SnapManager für Oracle

Die SnapManager-Befehlsreferenz enthält die gültige Syntax, Optionen, Parameter und Argumente, die Sie zusammen mit Beispielen mit den Befehlen bereitstellen sollten.

Die folgenden Probleme gelten für die Verwendung von Befehlen:

- Bei Befehlen wird die Groß-/Kleinschreibung beachtet.
- SnapManager akzeptiert bis zu 200 Zeichen und Labels mit bis zu 80 Zeichen.
- Wenn die Shell auf Ihrem Host die Anzahl der Zeichen begrenzt, die in einer Befehlszeile angezeigt werden können, können Sie den Befehl cmdfile verwenden.
- Verwenden Sie keine Leerzeichen in Profilnamen oder Namen.
- Verwenden Sie in der Klonspezifikation keine Leerzeichen am Klonspeicherort.

SnapManager kann drei Meldungsebenen in der Konsole anzeigen:

- Fehlermeldungen
- Warnmeldungen
- Informationsmeldungen

Sie können festlegen, wie Meldungen angezeigt werden sollen. Wenn Sie nichts angeben, wird in SnapManager nur Fehlermeldungen und Warnmeldungen an der Konsole angezeigt. Verwenden Sie eine der folgenden Befehlszeilenoptionen, um die Menge der Ausgabe, die SnapManager in der Konsole angezeigt wird:

- -Quiet: Zeigt nur Fehlermeldungen an der Konsole an.
- -Verbose: Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Unabhängig vom Standardverhalten oder der Detailebene, die Sie für die Anzeige angeben, schreibt SnapManager immer alle Nachrichtentypen in die Protokolldateien.

Der Befehl smo_Server restart

Mit diesem Befehl wird der SnapManager-Hostserver neu gestartet und als root eingegeben.

Syntax

```
        smo_server restart
[-quiet | -verbose]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen auf der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen auf der Konsole angezeigt werden.

Beispielbefehl

Im folgenden Beispiel wird der Host-Server neu gestartet.

```
smo_server restart
```

Der Befehl smo_Server Start

Mit diesem Befehl wird der Host-Server gestartet, auf dem die SnapManager für Oracle-Software ausgeführt wird.

Syntax

```
        smo_server start
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen auf der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen auf der Konsole angezeigt werden.

Beispielbefehl

Das folgende Beispiel startet den Host-Server.

```
smo_server start
SMO-17100: SnapManager Server started on secure port 25204 with PID 11250
```

Der Status-Befehl smo_Server

Sie können den smo_Server Status Befehl ausführen, um den Status des SnapManager Host Servers anzuzeigen.

Syntax

```
        smo_server status
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen in der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen in der Konsole angezeigt werden.

Beispiel

Im folgenden Beispiel wird der Status des Host-Servers angezeigt:

```
smo_server status
SMO-17104: SnapManager Server version 3.3.1 is running on secure port
25204 with PID 11250
  and has 0 operations in progress.
```

Der Befehl smo_Server stop

Dieser Befehl stoppt den SnapManager-Hostserver und wird im Root eingegeben.

Syntax

```
        smo_server stop
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen auf der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen auf der Konsole angezeigt werden.

Beispielbefehl

Im folgenden Beispiel wird der Befehl smo_Server stop verwendet.

```
smo_server stop
```

Der Befehl smo Backup erstellen

Sie können den Befehl Backup create ausführen, um Datenbank-Backups auf einem oder mehreren Speichersystemen zu erstellen.

Syntax

Bevor Sie diesen Befehl ausführen, müssen Sie ein Datenbankprofil mithilfe des Befehls Profile create erstellen erstellen.

```
        smo backup create
-profile profile_name
{\[-full\{-auto \| -online \| -offline\}\[-retain \{-hourly \| -daily \|
-weekly \| -monthly \| -unlimited\} \[-verify\]  |
\[-data \[\[-files files \[files\]\] \|
\[-tablespaces tablespaces \[tablespaces\]\] \[-label label\] \{-auto \|
-online \| -offline\}
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\} \[-
verify\] |
\[-archivelogs \[-label label\]\] \[-comment comment\]}
\[-protect \| -noprotect \| -protectnow\]
\[-backup-dest path1 \[ , path2\]\]
\[-exclude-dest path1 \[ , path2\]\]
\[-prunelogs \{-all \| -until-scn until-scn \| -until-date yyyy-MM-
dd:HH:mm:ss\] \| -before \{-months \| -days \| -weeks \| -hours}}
-prune-dest prune_dest1,\[prune_dest2\]\]
\[-taskspec taskspec\]
\[-dump\]
-force
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die gesichert werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Auto Option**

  Wenn die Datenbank im Status „angehängt“ oder „Offline“ steht, führt SnapManager ein Offline-Backup durch. Wenn sich die Datenbank im offenen oder Online-Status befindet, führt SnapManager ein Online-Backup durch. Wenn Sie die Option -Force mit der Option -offline verwenden, erzwingt SnapManager ein Offline-Backup, selbst wenn die Datenbank derzeit online ist.

- **-Online-Option**

  Gibt ein Online-Datenbank-Backup an.

  Sie können ein Online-Backup einer RAC-Datenbank (Real Application Clusters) erstellen, solange sich der primäre Status im offenen Zustand befindet oder der primäre Server gemountet ist und sich eine Instanz im offenen Zustand befindet. Sie können die Option -Force für Online-Backups verwenden, wenn sich die lokale Instanz im Shutdown-Status befindet, oder sich keine Instanz im offenen Status befindet. Die Version von Oracle muss 10.2.0.5 sein. Andernfalls wird die Datenbank hängen, wenn eine Instanz im RAC eingebunden ist.

  - Wenn sich die lokale Instanz im Status beim Herunterfahren befindet und sich mindestens eine Instanz im offenen Status befindet, können Sie die Option -Force verwenden, um die lokale Instanz in den angehängten Status zu ändern.
  - Wenn sich keine Instanz im Status „Open“ befindet, können Sie die Option „-Force“ verwenden, um die lokale Instanz in den Status „Open“ zu ändern.
- **-Offline-Option**

  Gibt ein Offline-Backup an, während sich die Datenbank im Status Herunterfahren befindet. Wenn sich die Datenbank im offenen oder gemounteten Status befindet, schlägt das Backup fehl. Wenn die Option -Force verwendet wird, versucht SnapManager, den Datenbankstatus zu ändern, um die Datenbank für ein Offline-Backup herunterzufahren.

- **-Volloption**

  Sicherung der gesamten Datenbank. Dazu gehören alle Daten, archivierte Log- und Kontrolldateien. Die archivierten Wiederherstellungsprotokolle und Kontrolldateien werden gesichert, unabhängig davon, welche Art von Backup Sie durchführen. Wenn Sie nur einen Teil der Datenbank sichern möchten, verwenden Sie die Option -files oder -Tablespaces.

- **-Datenoption**

  Gibt die Datendateien an.

- **-Dateiliste**

  Sichert nur die angegebenen Datendateien sowie die archivierten Protokoll- und Kontrolldateien. Trennen Sie die Liste der Dateinamen mit Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * -Tablespaces*

  Sicherung nur der angegebenen Datenbanktablespaces plus der archivierten Protokoll- und Kontrolldateien Trennen Sie die Namen der Tablespaces durch Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * Label*

  Gibt einen optionalen Namen für dieses Backup an. Dieser Name muss innerhalb des Profils eindeutig sein. Der Name kann Buchstaben, Zahlen, Unterstriche (_) und Bindestriche (-) enthalten. Es kann nicht mit einem Bindestrich beginnen. Wenn Sie keine Beschriftung angeben, erstellt SnapManager im Scope_type_date-Format eine Standardbeschriftung:

  - Der Umfang ist entweder F, um ein vollständiges Backup anzuzeigen, oder P, um auf ein teilweises

Backup hinzuweisen.

- Geben Sie C ein, um ein Offline-Backup (Cold) anzuzeigen, H für ein Online-Backup (Hot) oder Ein Für die automatische Sicherung, z. B. P_A_20081010060037IST, anzuzeigen.
- Datum ist Jahr, Monat, Tag und Uhrzeit des Backups.

  SnapManager verwendet eine 24-Stunden-Zeit.

Beispiel: Wenn Sie am 16. Januar 2007 um 5:45:16 Uhr eine vollständige Sicherung mit offline der Datenbank durchgeführt haben Eastern Standard Time, SnapManager würde die Bezeichnung F_C_20070116174516EST erstellen.

- **-comment-Zeichenfolge**

  Gibt einen optionalen Kommentar an, um dieses Backup zu beschreiben. Schließen Sie die Zeichenfolge in einzelne Anführungszeichen (').

  Einige Schalen entfernen die Anführungszeichen. In diesem Fall müssen Sie das Anführungszeichen mit einem umgekehrten Schrägstrich (\) angeben. Möglicherweise müssen Sie Folgendes eingeben: `\' this is a comment\'`.

- **-Verify Option**

  Überprüft, ob die Dateien im Backup nicht beschädigt sind, indem Sie das Oracle dbv-Dienstprogramm ausführen.

  Wenn Sie die Option -verify angeben, wird der Backup-Vorgang erst abgeschlossen, wenn der Überprüfungvorgang abgeschlossen ist.

- **-Force Option**

  Erzwingt eine Statusänderung, wenn sich die Datenbank nicht im richtigen Zustand befindet. Beispielsweise kann SnapManager den Status der Datenbank von Online- in Offline-Modus ändern, basierend auf dem von Ihnen angegebenen Backup-Typ und dem Status, in dem sich die Datenbank befindet.

  Verwenden Sie bei einem Online-Backup der RAC-Datenbank die Option -Force, wenn sich die lokale Instanz im Status Herunterfahren befindet, oder sich keine Instanz im offenen Status befindet.

  Die Version von Oracle muss 10.2.0.5 sein. Andernfalls wird die Datenbank hängen, wenn eine Instanz im RAC eingebunden ist.

  - Wenn sich die lokale Instanz im Status beim Herunterfahren befindet und sich mindestens eine Instanz im offenen Status befindet, wird die lokale Instanz mit der Option -Force in den angehängten Status geändert.
  - Wenn sich keine Instanz im Status Open befindet, wird die lokale Instanz mithilfe der Option -Force in den Status Open geändert.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

- * -Schutz *

  Gibt an, ob das Backup auf sekundärem Storage gesichert werden soll. Die Option -noprotect gibt an, dass das Backup nicht auf einem sekundären Speicher geschützt werden soll. Nur vollständige Backups sind gesichert. Wenn keine Option angegeben wird, schützt SnapManager das Backup standardmäßig, wenn es sich bei dem Backup um ein vollständiges Backup handelt, und das Profil eine Schutzrichtlinie angibt. Die Option -protectnow gilt nur für Data ONTAP im 7-Mode. Die Option gibt an, dass das Backup sofort auf dem sekundären Storage geschützt ist.

- **-halten Sie { - stündlich - jeden Tag — monatlich - unbegrenzt}**

  Gibt an, ob das Backup stündlich, täglich, wöchentlich, monatlich oder unbegrenzt aufbewahrt werden soll. Wenn die Option -Retention nicht angegeben ist, orientiert sich die Retention class standardmäßig an der Option -hourly. Mit der Option -unlimited können Sie Backups für immer aufbewahren. Die Option -unlimited macht das Backup nicht zur Löschung durch die Aufbewahrungsrichtlinie.

- **-Archivprotokolle-Option**

  Erstellt Backup für Archivprotokolle

- **-Backup-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll an, die für die Sicherung des Archivprotokolls gesichert werden sollen.

- **-exclude-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll an, die vom Backup ausgeschlossen werden sollen.

- *-prunelogs {-all} -bis-scnbis-scn - bis-dateyyyyy-MM-dd:HH:mm:ss - vor {-Monaten

  Löscht die Archivprotokolldateien aus den Zielen des Archivprotokolls basierend auf den bei der Erstellung eines Backups bereitgestellten Optionen. Die Option -all löscht alle Archivprotokolldateien aus den Archivprotokollzielen. Mit der Option -bis-scn werden die Archivprotokolldateien bis zu einer angegebenen Systemänderungsnummer (SCN) gelöscht. Mit der Option -bis-date werden die Archivprotokolldateien bis zum angegebenen Zeitraum gelöscht. Die Option -before löscht die Archivprotokolldateien vor dem angegebenen Zeitraum (Tage, Monate, Wochen, Stunden).

- **-prune-dest prune_dest1,prune_dest2**

  Löscht die Archivprotokolldateien aus den Archivprotokollzielen, während die Sicherung erstellt wird.

- **-taskSpec taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation an, die für die Vorverarbeitung oder Nachverarbeitung des Backup-Vorgangs verwendet werden kann. Der vollständige Pfad der XML-Datei sollte zur Verfügung gestellt werden, während die Option -taskSpec angegeben wird.

- **-dump-Option**

  Sammelt die Speicherauszugsdateien nach einem erfolgreichen oder fehlgeschlagenen Datenbanksicherungvorgang.

Beispielbefehl

Mit dem folgenden Befehl wird ein vollständiges Online Backup erstellt, ein Backup auf dem Sekundärspeicher erstellt und die Aufbewahrungsrichtlinie auf einen täglichen Routineaufgaben setzt:

```
smo backup create -profile SALES1 -full -online
-label full_backup_sales_May -profile SALESDB -force -retain -daily
Operation Id [8abc01ec0e79356d010e793581f70001] succeeded.
```

Verwandte Informationen

Datenbank-Backups werden erstellt

Der Befehl smo profile create

Wiederherstellen geschützter Backups aus dem sekundären Speicher

Der Befehl smo Backup delete

Sie können den Befehl zum Löschen von Backups ausführen, um Backups zu entfernen, die nicht automatisch entfernt werden, z. B. Backups, die zum Erstellen eines Klons oder einer fehlgeschlagenen Backups verwendet wurden. Sie können Backups, die unbegrenzt aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Syntax

```
        smo backup delete
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Datenbank an, die mit dem Backup verknüpft ist, das Sie entfernen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Gibt das Backup mit der angegebenen GUID an. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Gibt das Backup mit der angegebenen Bezeichnung an. Geben Sie optional den Umfang des Backups als

Datendatei oder Archivprotokoll an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-alle**

  Gibt alle Backups an. Verwenden Sie zum Löschen nur der angegebenen Backups die Option -id oder -Label.

- **-dump**

  Sammelt die Speicherauszugsdateien nach einem erfolgreichen oder fehlgeschlagenen Backup-Löschvorgang.

- **-Force**

  Erzwingt das Entfernen der Sicherung. SnapManager entfernt das Backup, selbst wenn es Probleme gibt, die mit dem Backup verbundenen Ressourcen freisetzen. Wenn das Backup beispielsweise mit dem Oracle Recovery Manager (RMAN) katalogisiert wurde, aber die RMAN-Datenbank nicht mehr existiert, einschließlich -Force löscht das Backup, obwohl es keine Verbindung mit RMAN herstellen kann.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Backup gelöscht:

```
smo backup delete -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Verwandte Informationen

Backups werden gelöscht

Der Befehl smo profile create

Der Befehl smoprofile Update

Der smo Backup kostenlose Befehl

Sie können den kostenlosen Befehl für die Sicherung ausführen, um die Snapshot-Kopien der Backups freizumachen, ohne die Backup-Metadaten aus dem Repository zu entfernen.

Syntax

```
        smo backup free
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, das mit dem Backup verknüpft ist, das Sie freigeben möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Gibt die Ressourcen des Backups mit der angegebenen GUID an. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen. Schließen Sie die -verbose Option zum Anzeigen der Backup-IDs an.

- * Label*

  Gibt das Backup mit der angegebenen Bezeichnung an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-alle**

  Gibt alle Backups an. Verwenden Sie zum Löschen der angegebenen Backups die Option -id oder -Label.

- **-Force**

  Erzwingt das Entfernen der Snapshot Kopien.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Das folgende Beispiel entlastet das Backup:

```
smo backup free -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Verwandte Informationen

So werden Backups entlastet

Der Befehl smo Backup list

Sie können den Befehl Backup list ausführen, um Informationen zu den Backups in einem Profil anzuzeigen, einschließlich Informationen zur Aufbewahrungsklasse und zum Sicherungsstatus.

Syntax

```
        smo backup list
-profile profile_name
-delimiter character
[-data | -archivelogs | -all]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie Backups auflisten möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Trennzeichen**

  Zeigt jede Zeile in einer eigenen Zeile an. Die Attribute in der Zeile werden durch das angegebene Zeichen getrennt.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an. Schließen Sie die -verbose Option zum Anzeigen der Backup-IDs an.

Beispiel

Im folgenden Beispiel werden die Backups für DAS SALES1-Profil aufgeführt:

```
smo backup list -profile SALES1 -verbose
Start Date          Status  Scope  Mode    Primary  Label      Retention
Protection
------------------- ------- ------ ------- -------- -----      --------
----------
2007-08-10 14:31:27 SUCCESS FULL   ONLINE  EXISTS   backup1    DAILY
PROTECTED
2007-08-10 14:12:31 SUCCESS FULL   ONLINE  EXISTS   backup2    HOURLY
NOT PROTECTED
2007-08-10 10:52:06 SUCCESS FULL   ONLINE  EXISTS   backup3    HOURLY
PROTECTED
2007-08-05 12:08:37 SUCCESS FULL   ONLINE  EXISTS   backup4    UNLIMITED
NOT PROTECTED
2007-08-05 09:22:08 SUCCESS FULL   OFFLINE EXISTS   backup5    HOURLY
PROTECTED
2007-08-04 22:03:09 SUCCESS FULL   ONLINE  EXISTS   backup6    UNLIMITED
NOT REQUESTED
2007-07-30 18:31:05 SUCCESS FULL   OFFLINE EXISTS   backup7    HOURLY
PROTECTED
```

Verwandte Informationen

Anzeigen einer Liste von Backups

Der Befehl smo Backup Mount

Sie können den Befehl Backup Mount ausführen, um ein Backup anzuhängen, um einen Wiederherstellungsvorgang mit einem externen Tool durchzuführen.

Syntax

```
        smo backup mount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
[-host  host]
\[-from-secondary \{-copy-id id\}\]
\[-dump\]
[-quiet | -verbose]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, das mit dem Backup verknüpft ist, das Sie mounten möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Bindet das Backup mit der angegebenen GUID ein. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Bindet das Backup mit dem angegebenen Etikett an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-from-secondary -copy-id**

  Bindet das Backup aus dem sekundären Storage ein Wenn diese Option nicht angegeben wird, bindet SnapManager das Backup vom primären Storage ein. Sie können diese Option bei der Freigabe des Backups verwenden.

  Sie müssen die Option -copy-id angeben, wenn Sie die Option -from-secondary angeben. Wenn mehrere Backups auf dem sekundären Speichersystem vorhanden sind, wird mit der Option -copy-id angegeben, welche Sicherungskopie auf dem sekundären Speicher zum Mounten des Backups verwendet werden soll.

  Wenn Sie Data ONTAP in 7-Mode verwenden, müssen Sie einen gültigen Wert für die Option -copy-id angeben. Wenn Sie jedoch Clustered Data ONTAP verwenden, ist die Option -copy-id nicht erforderlich.

- * Host*

  Gibt den Host an, auf dem das Backup gemountet werden soll.

- **-dump**

Sammelt die Speicherauszugsdateien nach dem erfolgreichen oder fehlgeschlagenen Mount-Vorgang.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

> Sie müssen diesen Befehl nur verwenden, wenn Sie ein externes Tool wie Oracle Recovery Manager (RMAN) verwenden. SnapManager übernimmt automatisch das Mounten von Backups, wenn Sie den smom Backup Restore Befehl verwenden, um das Backup wiederherzustellen. Mit diesem Befehl wird eine Liste angezeigt, die die Pfade anzeigt, auf denen die Snapshot Kopien angehängt wurden. Diese Liste wird nur angezeigt, wenn die Option -verbose angegeben ist.

Beispiel

Das folgende Beispiel hängt den Backup ab:

```
smo backup mount -profile SALES1 -label full_backup_sales_May -verbose
SMO-13046 [INFO ]: Operation GUID 8abc013111b9088e0111b908a7560001
starting on Profile SALES1
SMO-08052 [INFO ]: Beginning to connect mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/logs from
snapshot SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_logs.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/logs from snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_logs.
SMO-08025 [INFO ]: Beginning to connect mount /mnt/ssys1/data from
snapshot SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of
volume hs_data.
SMO-08027 [INFO ]: Finished connecting mount /mnt/ssys1/data from snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_data.
SMO-08053 [INFO ]: Finished connecting mount(s) [/mnt/ssys1/logs,
/mnt/ssys1/data] from logical snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001.
SMO-13037 [INFO ]: Successfully completed operation: Backup Mount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:01:00.981
Operation Id [8abc013111b9088e0111b908a7560001] succeeded.
```

Verwandte Informationen

Montage von Backups

Der Smo Backup Restore Befehl

Sie können den Befehl Backup Restore ausführen, um Backups einer Datenbank oder eines Teils einer Datenbank wiederherzustellen, und optional die Datenbankinformationen wiederherstellen.

Syntax

```
        smo backup restore
-profile profile_name
\[-label label \| -id id\]
\[-files files \[files...\] \|
-tablespaces tablespaces \[tablespaces...\]\] \|
-complete \| -controlfiles\]
\[-recover \{-alllogs \| -nologs \| -until until\} \[-using-backup-
controlfile\] \]
\[-restorespec restorespec \| -from-secondary \[-temp-volume temp_volume\]
\[-copy-id id\]\]
\[-preview\]
\[-fast \{-require \| -override \| -fallback \| -off\}\]
\[-recover-from-location path1 \[, path2\]\]
\[-taskspec taskspec\]
\[-dump\]
\[-force\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Datenbank an, die wiederhergestellt werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- * Name des Etiketts*

  Stellt das Backup mit dem angegebenen Etikett wieder her.

- **-id-Guid**

  Stellt die Sicherung mit der angegebenen GUID wieder her. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- **Wählen Sie alle oder bestimmte Dateien**

Optional können Sie eine der folgenden Optionen verwenden:

- -Complete: Stellt alle Dateien in der Sicherung wieder her.
- -Tablespaceslist: Stellt nur die angegebenen Tablespaces aus dem Backup wieder her.

  Sie müssen Leerzeichen verwenden, um die Namen in der Liste zu trennen.

- -Fileslist: Stellt nur die angegebenen Datendateien aus dem Backup wieder her.

  Sie müssen Leerzeichen verwenden, um die Namen in der Liste zu trennen. Wenn die Datenbank ausgeführt wird, stellt SnapManager sicher, dass der Tablespace, der die Dateien enthält, offline ist.

- **-controlfiles**

  Stellt die Kontrolldateien wieder her. SnapManager ermöglicht Ihnen, in einem einzigen Vorgang Kontrolldateien zusammen mit den Datendateien aus den Backups wiederherzustellen. Die Option -controlfiles ist unabhängig von anderen Parametern für den Wiederherstellungsumfang, wie z. B. -Complete, -Tablespaces und -Files.

- **-Erholung**

  Stellt die Datenbank nach der Wiederherstellung wieder her. Sie müssen auch den Punkt angeben, an dem SnapManager die Datenbank wiederherstellen soll, indem Sie eine der folgenden Optionen verwenden:

  - -Nologs: Stellt die Datenbank zum Zeitpunkt der Sicherung wieder her und wendet keine Logs an.

    Sie können diesen Parameter für Online- oder Offline-Backups verwenden.

  - -Alllogs: Stellt die Datenbank auf die letzte Transaktion oder Commit wieder her und wendet alle erforderlichen Protokolle an.
  - -Bis Datum: Stellt die Datenbank bis zum angegebenen Datum und der angegebenen Zeit wieder her.

    Sie müssen das Jahr-Monat-Datum verwenden: Stunde: Minute: Sekunde (yyyy-mm-dd:hh:mm:ss) Format. Verwenden Sie für Stunden je nach Datenbankeinstellung entweder das 12-Stunden- oder das 24-Stunden-Format.

  - -Bis scn: Rollt die Datendateien weiter, bis sie die angegebene Systemändernummer (SCN) erreicht.
  - -Using-Backup-controlfile: Stellt die Datenbank mit der Backup-Kontrolldatei wieder her.

- **-restaurespec**

  Ermöglicht Ihnen, die Daten in einem aktiven File-System wiederherzustellen und aus den angegebenen Daten wiederherzustellen, indem Sie jede Original-Snapshot-Kopie einem aktiven File-System zuweisen. Falls Sie keine Option angeben, werden die Daten aus den Snapshot Kopien im primären Storage von SnapManager wiederhergestellt. Sie können eine der folgenden Optionen angeben:

  - -Restorespec: Gibt die wiederherzustellenden Daten und das Wiederherstellungsformat an.
  - -Aus dem sekundären: Stellt die Daten aus dem sekundären Speicher wieder her.

    Diese Option kann nicht verwendet werden, wenn das Backup im Primär-Storage vorhanden ist. Das primäre Backup muss freigegeben werden, bevor ein Backup aus dem sekundären Storage wiederhergestellt werden kann. Wenn Sie ein temporäres Volumen verwenden, müssen Sie das Volumen mithilfe der Option -temp-Volume angeben.

Sie müssen die Option -copy-id angeben, wenn Sie die Option -from-secondary angeben. Wenn auf dem sekundären Speichersystem mehrere Backups vorhanden sind, wird mit der Option -copy-id angegeben, welche Backup-Kopie auf dem sekundären Speicher für den Wiederherstellungsvorgang verwendet werden soll.

Wenn Sie Data ONTAP in 7-Mode verwenden, müssen Sie einen gültigen Wert für die Option -copy-id angeben. Wenn Sie jedoch Clustered Data ONTAP verwenden, ist die Option -copy-id nicht erforderlich

Bei der Wiederherstellung aus dem Sekundärspeicher versucht SnapManager zunächst, Daten direkt aus dem sekundären Speichersystem auf das primäre Speichersystem (ohne Beteiligung des Hosts) wiederherzustellen. Wenn SnapManager diese Art der Wiederherstellung nicht durchführen kann (z. B. wenn die Dateien nicht Teil des Dateisystems sind), dann wird SnapManager zurück zu einer Host-seitigen Dateikopie zurückkehren. SnapManager verfügt über zwei Methoden zur Wiederherstellung einer Host-seitigen Dateikopie aus dem sekundären Server. Die von SnapManager gewählte Methode wird in der smo.config-Datei konfiguriert.

- Direkt: SnapManager klont die Daten auf sekundärem Storage, mountet die geklonten Daten vom sekundären Storage-System auf den Host und kopiert sie dann Daten aus dem Klon in die aktive Umgebung.

  Dies ist die standardmäßige sekundäre Zugriffsrichtlinie.

- Indirekt: SnapManager kopiert die Daten zunächst auf ein temporäres Volume im Primärspeicher, bindet die Daten vom temporären Volume an den Host und kopiert dann Daten aus dem temporären Volume in die aktive Umgebung.

  Diese Richtlinie sollte nur verwendet werden, wenn der Host keinen direkten Zugriff auf das sekundäre Speichersystem hat. Wiederherstellungen mit der indirekten Methode dauern doppelt so lange wie die Richtlinien für direkte sekundäre Zugriffe, da zwei Kopien der Daten erstellt werden.

Die Entscheidung, ob die direkte oder indirekte Methode verwendet werden soll, wird durch den Wert des Parameters restore.secondaryAccessPolicy in der Konfigurationsdatei smo.config gesteuert.

- * Vorschau*

  Zeigt die folgenden Informationen an:

  - Welcher Wiederherstellungsmechanismus (schnelle Wiederherstellung, Filesystem-Wiederherstellung auf Storage-Seite, Dateiwiederherstellung auf Storage-Seite oder Wiederherstellung von Host-seitigen Dateikopien) wird zum Wiederherstellen jeder Datei verwendet
  - Warum effizientere Mechanismen nicht zur Wiederherstellung jeder Datei verwendet wurden, wenn Sie die Option -verbose angeben Wenn Sie die Option -Preview verwenden, müssen Sie Folgendes wissen:
  - Die Option -Force hat keine Auswirkung auf den Befehl.
  - Die Option -wiederherstellen hat keine Auswirkung auf den Befehl.
  - Die Option -fast (-enterride, -override, -Fallback oder -off) hat erhebliche Auswirkungen auf die Ausgabe. Um eine Vorschau des Wiederherstellungsvorgangs anzuzeigen, muss die Datenbank gemountet werden. Wenn Sie eine Vorschau eines Wiederherstellungsplans anzeigen möchten und die Datenbank derzeit nicht angehängt ist, mountet SnapManager die Datenbank. Wenn die Datenbank nicht angehängt werden kann, schlägt der Befehl fehl, und SnapManager gibt die Datenbank in ihren ursprünglichen Status zurück.

Die Option -Preview zeigt bis zu 20 Dateien an. Sie können die maximale Anzahl von Dateien konfigurieren, die in der Datei smo.config angezeigt werden sollen.

- **-schnell**

  Ermöglicht Ihnen die Auswahl des Prozesses, den Sie für den Wiederherstellungsvorgang verwenden möchten. Zudem kann SnapManager die Verwendung des Volume-basierten schnellen Wiederherstellungsprozesses anstelle anderer Wiederherstellungsverfahren erzwingen, wenn alle obligatorischen Bedingungen für die Wiederherstellung erfüllt sind. Falls bekannt ist, dass eine Wiederherstellung eines Volumes nicht möglich ist, kann dieser Vorgang ebenfalls durchgeführt werden, um SnapManager die Überprüfung der Berechtigung und die Wiederherstellung mithilfe des schnellen Restore-Vorgangs zu verhindern.

  Die Option -fast umfasst die folgenden Parameter:

  - -Erforderlich: Ermöglicht es Ihnen, SnapManager zu zwingen, eine Volume-Wiederherstellung durchzuführen, wenn alle Bedingungen für die Wiederherstellung erfüllt sind.

    Wenn Sie die Option -fast angeben, jedoch keinen Parameter für -fast angeben, verwendet SnapManager als Standard den Parameter -erfordern.

  - -Override: Ermöglicht es Ihnen, die nicht obligatorischen Eignungsprüfungen zu überschreiben und den volumenbasierten schnellen Wiederherstellungsprozess durchzuführen.
  - -Fallback: Ermöglicht es Ihnen, die Datenbank mit jeder Methode wiederherzustellen, die SnapManager bestimmt.

    Wenn Sie die Option -fast nicht angeben, verwendet SnapManager die standardmäßige Option Backup restore -fast Fallback.

  - -Off: Ermöglicht Ihnen, die Zeit zu vermeiden, die für die Durchführung von Eignungsprüfungen erforderlich ist.
- **-Recovery-from-location**

  Gibt den externen Speicherort der Archivprotokolldateien an. SnapManager nimmt die Archivprotokolldateien vom externen Standort auf und verwendet diese für den Recovery-Prozess.

- **-taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation für die Vorverarbeitung oder Nachbearbeitung des Wiederherstellungsvorgangs an. Sie müssen den vollständigen Pfad der XML-Datei für die Aufgabenspezifikation angeben.

- **-dump**

  Gibt an, die Speicherauszugsdateien nach dem Wiederherstellungsvorgang zu sammeln.

- **-Force**

  Ändert ggf. den Datenbankstatus in einen niedrigeren Status als der aktuelle Status. Für Real Application Clusters (RAC) müssen Sie die Option -Force angeben, wenn SnapManager den Status einer beliebigen RAC-Instanz in einen niedrigeren Status ändern muss.

  Standardmäßig kann SnapManager den Datenbankstatus während eines Vorgangs in einen höheren Status ändern. Diese Option ist nicht erforderlich, damit SnapManager die Datenbank in einen höheren Status ändert.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an. Sie können diese Option verwenden, um zu sehen, warum effizientere Wiederherstellungsprozesse nicht verwendet werden konnten, um die Datei wiederherzustellen.

Beispiel

Im folgenden Beispiel wird eine Datenbank zusammen mit den Kontrolldateien wiederhergestellt:

```
smo backup restore -profile SALES1 -label full_backup_sales_May
-complete -controlfiles -force
```

Verwandte Informationen

Datenbank-Backups werden wiederhergestellt

Wiederherstellen von Backups von einem alternativen Speicherort

Erstellen von Wiederherstellungsspezifikationen

Der Befehl smo Backup show

Mit dem Befehl Backup show können Sie detaillierte Informationen zu einem Backup anzeigen, einschließlich Sicherungsstatus, Backup-Aufbewahrungsklasse und Backups im primären und sekundären Speicher.

Syntax

```
        smo backup show
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Backups angezeigt werden sollen. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- * Label*

  Gibt die Bezeichnung des Backups an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-id-id**

  Gibt die Backup-ID an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen der Konsole sowie Klon- und Verifizierungsdaten an.

Beispiel

Im folgenden Beispiel werden ausführliche Informationen zum Backup angezeigt:

```
smo backup show -profile SALES1 -label BTNFS -verbose
Backup id: 8abc013111a450480111a45066210001
Backup status: SUCCESS
Primary storage resources: EXISTS
Protection sate: PROTECTED
Retention class: DAILY
Backup scope: FULL
Backup mode: OFFLINE
Mount status: NOT MOUNTED
Backup label: BTNFS
Backup comment:
RMAN Tag: SMO_BTNFS_1175283108815
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Verification status: OK
Backup Retention Policy: NORMAL
Backup database: hsdb1
Checkpoint: 2700620
Tablespace: SYSAUX
Datafile: /mnt/ssys1/data/hsdb/sysaux01.dbf [ONLINE]
...
Control Files:
File: /mnt/ssys1/data/control03.ctl
...
Archive Logs:
File: /mnt/ssys1/data/archive_logs/2_131_626174106.dbf
...
Host: Host1
Filesystem: /mnt/ssys1/data
File: /mnt/ssys1/data/hsdb/SMOBakCtl_1175283005231_0
...
Volume: hs_data
Snapshot: SMO_HSDBR_hsdb1_F_C_1_
8abc013111a450480111a45066210001_0
File: /mnt/ssys1/data/hsdb/SMOBakCtl_1175283005231_0
...
Protected copies on Secondary Storage:
  14448939 - manow
  88309228 - graffe
```

Verwandte Informationen

Anzeigen von Backup-Details

Der Befehl smo Backup unmount

Sie können den Befehl Backup unmount ausführen, um die Bereitstellung eines Backups zu aufheben.

Syntax

```
        smo backup unmount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das die Bereitstellung eines Backups aufgehoben werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-id**

  Hängt das Backup mit der angegebenen GUID ab. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Hängt das Backup mit dem angegebenen Etikett ab.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-dump**

  Sammelt die Speicherauszugsdateien nach einem erfolgreichen oder fehlgeschlagenen Aushängevorgang.

- **-Force**

  Hängt das Backup ab, selbst wenn beim Freigeben der mit dem Backup verbundenen Ressourcen Probleme auftreten. SnapManager versucht, die Bereitstellung des Backups rückgängig zu machen und die zugehörigen Ressourcen zu bereinigen. Das Protokoll zeigt den Vorgang zum Aufheben der Bereitstellung als erfolgreich an. Bei Fehlern im Protokoll müssen Sie jedoch möglicherweise Ressourcen manuell bereinigen.

- **-ruhig**

Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im Folgenden finden Sie ein Beispiel für einen unmontierten Vorgang:

```
# smo backup unmount -label test -profile SALES1 -verbose
```

```
SMO-13046 [INFO ]: Operation GUID 8abc013111b909eb0111b90a02f50001
starting on Profile SALES1
SMO-08028 [INFO ]: Beginning to disconnect connected mount(s)
[/u/user1/mnt/_mnt_ssys1_logs_SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a
45066210001,
 /u/user1/mnt/_mnt_ssys1_data_SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a
45066210001].
SMO-08030 [INFO ]: Done disconnecting connected mount(s)
[/u/user1/mnt/_mnt_ssys1_logs_SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a
45066210001,
 /u/user1/mnt/_mnt_ssys1_data_SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a
45066210001].
SMO-13037 [INFO ]: Successfully completed operation: Backup Unmount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:00:33.715
Operation Id [8abc013111b909eb0111b90a02f50001] succeeded.
```

Verwandte Informationen

UnMounten von Backups

Der SMO-Befehl zum Aktualisieren der Datensicherung

Sie können den Befehl Backup Update ausführen, um die Backup-Aufbewahrungsrichtlinie zu aktualisieren.

Syntax

```
        smo backup update
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-comment comment_text\]
[-quiet | -verbose]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Backups aktualisiert werden sollen. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Überprüft die Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Gibt das Backup-Label und den Umfang des Backups als Datendatei oder Archivprotokoll an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-comment comment comment_Text**

  Geben Sie Text (bis zu 200 Zeichen) zum Backup-Update ein. Sie können Leerzeichen einschließen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

- **-halten Sie {-stündlich / -täglich / -monatlich / -unbegrenzt}**

  Gibt an, ob das Backup stündlich, täglich, wöchentlich, monatlich oder unbegrenzt aufbewahrt werden soll. Wenn -Retention nicht angegeben ist, wird die Aufbewahrungsklasse standardmäßig auf -hourly gesetzt. Mit der Option -unlimited können Sie Backups für immer aufbewahren. Die Option -unlimited macht das Backup nicht zum Löschen.

Beispiel

Im folgenden Beispiel wird das Backup aktualisiert, damit die Aufbewahrungsrichtlinie auf unbegrenzt gesetzt wird:

```
smo backup update -profile SALES1 -label full_backup_sales_May
-retain -unlimited -comment save_forever_monthly_backup
```

Verwandte Informationen

Ändern der Richtlinie zur Aufbewahrung von Backups

Dauerhaft Aufbewahrung von Backups

Freistellen oder Löschen von Backups ohne Rücknahmerichtlinien

Der Befehl smo Backup verify

Sie können den Befehl Backup Verify ausführen, um festzustellen, ob sich das Backup in einem gültigen Format für Oracle befindet.

Syntax

```
        smo backup verify
-profile profile_name
[-label backup_name \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie ein Backup überprüfen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Überprüft die Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- **-Label Label Label_Name**

  Überprüfung der Sicherung mit der angegebenen Bezeichnung.

- **-dump**

Sammelt die Speicherauszugsdateien nach dem erfolgreichen oder fehlgeschlagenen Backup-Überprüfungvorgang.

- **-Force**

  Erzwingt die Datenbank in den erforderlichen Zustand, um den Verifizierungsvorgang durchzuführen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Das folgende Beispiel zeigt die Überprüfung des Backups:

```
smo backup verify -profile SALES1 -label full_backup_sales_May -quiet
```

```
DBVERIFY - Verification starting : FILE =
+SMO_1_1161675083835/smo/datafile/data.277.582482539 ...
```

Verwandte Informationen

Datenbank-Backups werden überprüft

Der Befehl Smo Clone create

Sie können den Befehl Clone create ausführen, um einen Klon einer gesicherten Datenbank zu erstellen. Sie können ein Backup aus primärem oder sekundärem Storage klonen.

Syntax

```
        smo clone create
-profile profile_name
[-backup-id backup_guid \| -backup-label backup_label_name \| -current\]
-newsid new_sid
\[-host target_host\]
[-label clone_label]
\[-comment string\]
-clonespec full_path_to_clonespec_file
\[-asminstance -asmusername asminstance_username  -asmpassword
asminstance_password\]]
\[-syspassword syspassword\]
\[-reserve \{yes \| no \| inherit\}\]
\[-from-secondary \{-copy-id id\}\]
\[-no-resetlogs \| -recover-from-location path1 \[, path2\]\]\[-taskspec
taskspec\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profilname**

  Gibt die Datenbank an, die geklont werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Backup-id Guid**

  Klont die Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list-verbose verwenden, um die GUID für jedes Backup anzuzeigen.

- **-Backup-Label Backup_Label_Name**

  Gibt an, dass das Backup mit dem angegebenen Namen geklont wird.

- **-Strom**

  Gibt an, dass Backup und Klon im aktuellen Status der Datenbank erstellt werden.

  > Wenn sich die Datenbank im Noarchivlog Modus befindet, wird SnapManager ein offline Backup erstellen.

- **-newsid New_sid**

  Gibt eine neue, eindeutige Oracle-Systemkennung für die geklonte Datenbank an. Der Wert für die Systemkennung darf maximal acht Zeichen lang sein. Oracle erlaubt nicht, zwei Datenbanken mit derselben Systemkennung auf demselben Host gleichzeitig auszuführen.

- **-Host target_Host**

Gibt den Host an, auf dem der Klon erstellt werden soll.

- **-Label Clone_Label**

  Gibt eine Bezeichnung für den Klon an.

- **-comment-Zeichenfolge**

  Gibt einen optionalen Kommentar an, um diesen Klon zu beschreiben. Sie müssen den String in einzelne Anführungszeichen einschließen.

  > Einige Shells löschen die Anführungszeichen. Wenn das für Ihre Shell gilt, müssen Sie dem Angebot mit einem umgekehrten Schrägstrich (\) entkommen. Beispiel: \' Dies ist ein Kommentar\'

- **-clonespec full_path_to_clonespec_file**

  Gibt den Pfad zur XML-Datei für die Klonspezifikation an. Dies kann ein relativer oder ein absoluter Pfadname sein.

- **-asminstance**

  Gibt die Anmeldeinformationen an, die zur Anmeldung bei der ASM-Instanz verwendet werden.

- **-asmusername asminstance_username**

  Gibt den Benutzernamen an, der zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-asmpassword asminstance_password**

  Gibt das Kennwort an, das zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-syspassword-syspassword**

  Gibt das Kennwort für den Benutzer mit Systemprivilegierten an.

  > Sie müssen das Passwort für den Benutzer mit Systemberechtigungen angeben, wenn die angegebenen Datenbankanmeldeinformationen nicht für den Benutzer mit Systemprivilegierten identisch sind.

- **-Reserve**

  Wenn Sie die Option -Reserve auf ja einstellen, wird sichergestellt, dass die Speicherplatzreserve für die neuen Klon-Volumes aktiviert ist. Wenn die Option -Reserve auf Nein eingestellt wird, wird sichergestellt, dass die Speicherplatzreserve für die neuen Klon-Volumes deaktiviert ist. Durch Festlegen der Option -Reserve wird sichergestellt, dass der neue Klon die Eigenschaften der Platzreservierung der übergeordneten Snapshot Kopie übernimmt. Die Standardeinstellung ist Nein

  In der folgenden Tabelle werden die Klonmethoden und ihre Auswirkung auf den Vorgang zum Erstellen von Klonen und seine Option -Reserve beschrieben. Eine LUN kann mit beiden Methoden geklont werden.

Klonmethode	Beschreibung	Ergebnis

LUN cloning	A new clone LUN is created within the same volume.	When the -reserve option for a LUN is set to yes, space is reserved for the full LUN size within the volume.
Volume cloning	A new FlexClone is created, and the clone LUN exists within the new clone volume. Uses the FlexClone technology.	When the -reserve option for a volume is set to yes, space is reserved for the full volume size within the aggregate. +

- **-from-secondary [-copy-idcopy_id]**

  Gibt an, dass SnapManager eine Kopie eines Backups klonen sollte, das zum sekundären Storage gesichert ist. Wenn diese Option nicht angegeben wird, klont SnapManager die Kopie aus dem primären Storage.

  Sie müssen die Option -copy-id angeben, wenn Sie die Option -from-secondary angeben. Wenn auf dem sekundären Speichersystem mehrere Backups vorhanden sind, wird mit der Option -copy-id angegeben, welche Backup-Kopie auf dem sekundären Speicher zum Klonen verwendet werden soll.

  Wenn Sie Data ONTAP in 7-Mode verwenden, müssen Sie einen gültigen Wert für die Option -copy-id angeben. Wenn Sie jedoch Clustered Data ONTAP verwenden, ist die Option -copy-id nicht erforderlich.

- **-no-resetlogs**

  Gibt an, die Wiederherstellung der Datenbank zu überspringen, das DBNEWID Dienstprogramm auszuführen und nicht die Datenbank mit den Resetlogs während der Erstellung des Klons zu öffnen.

- **-Recovery-from-location**

  Gibt den externen Speicherort für das Archivprotokoll an, an dem SnapManager die Archivprotokolldateien vom externen Speicherort übernimmt und zum Klonen verwendet.

- **-taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation für die Vorverarbeitung oder Nachverarbeitung des Klonvorgangs an. Sie müssen den vollständigen Pfad der XML-Datei für die Aufgabenspezifikation angeben.

- **-dump**

  Gibt an, die Dump-Dateien nach dem Erstellungsvorgang des Klons zu sammeln.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Backup mit einer Klonspezifikation geklont, die für diesen Klon erstellt wird:

```
smo clone create -profile SALES1 -backup-label full_backup_sales_May
-newsid
CLONE -label sales1_clone -clonespec
/opt/<path>/smo/clonespecs/sales1_clonespec.xml
```

```
Operation Id [8abc01ec0e794e3f010e794e6e9b0001] succeeded.
```

Verwandte Informationen

Erstellen von Klonspezifikationen

Klonen von Datenbanken aus Backups

Der Befehl smo Clone delete

Sie können den Befehl „Klon löschen“ ausführen, um einen Klon zu löschen. Sie können einen Klon nicht löschen, wenn der Klon für einen Vorgang verwendet wird.

Syntax

```
        smo clone delete
-profile profile_name
\[-id guid \| -label clone_name\]
[-login
\[-username db_username -password db_password -port db_port\]
 \[-asminstance -asmusername asminstance_username  -asmpassword
asminstance_password\]]
\[-syspassword syspassword\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das den zu löschenden Klon enthält. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Force**

  Löscht den Klon, auch wenn dem Klon Ressourcen zugeordnet sind.

- **-id-Guid**

  Gibt die GUID für den zu löschenden Klon an. Die GUID wird von SnapManager beim Erstellen eines Klons generiert. Sie können den Befehl smo Clone list verwenden, um die GUID für jeden Klon anzuzeigen.

- * Name des Etiketts*

  Gibt die Bezeichnung für den zu löschenden Klon an.

- **-asminstance**

  Gibt die Anmeldeinformationen an, die zur Anmeldung bei der Instanz für die automatische Speicherverwaltung (ASM) verwendet werden.

- **-asmusername asminstance_username**

  Gibt den Benutzernamen an, der zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-asmpassword asminstance_password**

  Gibt das Kennwort an, das zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-syspassword-syspassword**

  Gibt das Kennwort für den Benutzer mit Systemprivilegierten an.

Sie müssen das Passwort für den Benutzer mit Systemberechtigungen angeben, wenn die angegebenen Datenbankanmeldeinformationen nicht für den Benutzer mit Systemprivilegierten identisch sind.

- **-Login**

  Ermöglicht die Eingabe der Anmeldedaten für die Datenbank.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist.

- **-Port db_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, die das Profil beschreibt.

- **-dump**

  Gibt an, die Speicherauszugsdateien nach dem Löschen des Klons zu sammeln.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird der Klon gelöscht:

```
smo clone delete -profile SALES1 -label SALES_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Der Befehl smo Clone list

Dieser Befehl listet die Klone der Datenbank für ein bestimmtes Profil auf.

Syntax

```
        smo clone list
-profile profile_name
-delimiter character
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Liste der mit dem Profil verknüpften Klone an. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Trennzeichen**

  Wenn dieser Parameter angegeben wird, führt der Befehl die Attribute in jeder Zeile durch das angegebene Zeichen getrennt auf.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden die Datenbankklone im SALES1-Profil aufgeführt.

```
smo clone list -profile SALES1 -verbose
```

```
ID Status SID Host Label Comment
-------- ------- ----- ------- ---------- -------
8ab...01 SUCCESS hsdbc server1 back1clone test comment
```

Verwandte Informationen

Anzeigen einer Liste von Klonen

Der Befehl smo Clone show

Sie können den Befehl Clone show ausführen, um Informationen über die Datenbankklone für das angegebene Profil anzuzeigen.

Syntax

```
        smo clone show
-profile profile_name
\[-id  guid \| -label clone_name\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Liste der mit dem Profil verknüpften Klone an. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Zeigt Informationen über den Klon mit der angegebenen GUID an. Die GUID wird von SnapManager beim Erstellen eines Klons generiert. Sie können den Befehl „smo Clone show“ verwenden, um die GUID für jeden Klon anzuzeigen.

- **-Label Label Label_Name**

  Zeigt Informationen über den Klon mit der angegebenen Bezeichnung an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel werden Informationen über den Klon angezeigt:

```
smo clone show -profile SALES1 -label full_backup_sales_May -verbose
```

Die folgende Ausgabe zeigt Informationen zu einem Backup-Klon des primären Storage:

```
Clone id: 8abc013111b916e30111b916ffb40001
Clone status: SUCCESS
Clone SID: hsdbc
Clone label: hsdbc
Clone comment: null
Clone start time: 2007-04-03 16:15:50
Clone end time: 2007-04-03 16:18:17
Clone host: Host1
Filesystem: /mnt/ssys1/data_clone
File: /mnt/ssys1/data_clone/hsdb/sysaux01.dbf
File: /mnt/ssys1/data_clone/hsdb/undotbs01.dbf
File: /mnt/ssys1/data_clone/hsdb/users01.dbf
File: /mnt/ssys1/data_clone/hsdb/system01.dbf
File: /mnt/ssys1/data_clone/hsdb/undotbs02.dbf
Backup id: 8abc013111a450480111a45066210001
Backup label: full_backup_sales_May
Backup SID: hsdb1
Backup comment:
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Backup host: server1
```

In der folgenden Ausgabe werden Informationen über einen Klon eines geschützten Backups im sekundären Storage angezeigt:

```
clone show -label clone_CLSTEST -profile
TEST_USER_NFSTEST_DIRMAC
Clone id:8abc01ec16514aec0116514af52f0001
Clone status: SUCCESS
Clone SID: CLSTEST
Clone label: clone_CLSTEST
Clone comment:comment_for_clone_CLSTEST
Clone start time: 2007-11-18 00:46:10
Clone end time: 2007-11-18 00:47:54
Clone host: dirmac
Filesystem: /ant/fish/bt_dirmac_nfs_clone
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/sysaux01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/system01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/undotbs01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/users01.dbf
Backup id: 8abc01ec16514883011651488b580001
Backup label:full_backup
Backup SID: NFSTEST
Backup comment:
Backup start time: 2007-11-18 00:43:32
Backup end time: 2007-11-18 00:45:30
Backup host: dirmac
Storage System: fish (Secondary storage)
Volume: bt_dirmac_nfs
Snapshot:smo_user_nfstest_b_nfstest_f_c_1_8abc01ec16511d6a0116511d73590001
_0
File: /ant/fish/bt_dirmac_nfs/archlogs/1_14_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/sysaux01.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/undotbs01.dbf
File: /ant/fish/bt_dirmac_nfs/archlogs/1_13_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/archlogs_2/1_16_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/users01.dbf
File: /ant/fish/bt_dirmac_nfs/controlfiles/SMBakCtl_1195361899651_2
File: /ant/fish/bt_dirmac_nfs/datafiles/system01.dbf
```

Verwandte Informationen

Anzeigen detaillierter Kloninformationen

Der Befehl smo Clone template

Mit diesem Befehl können Sie eine Vorlage für die Klonspezifikation erstellen.

Syntax

```
        smo clone template
-profile name
\[-backup-id guid  \| -backup-label backup_name\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profilname**

  Gibt die Datenbank an, für die Sie eine Klonspezifikation von erstellen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Backup-id Guid**

  Erstellt eine Klonspezifikation aus der Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Verwenden Sie den Befehl smo Backup list, um die GUID für jedes Backup anzuzeigen.

- **-Backup-Label Backup_Label_Name**

  Erstellt eine Klonspezifikation aus der Sicherung mit dem angegebenen Backup-Label.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel wird aus dem Backup eine Klon-Spezifikations-Vorlage mit dem Label full_Backup_Sales_May erstellt. Sobald der Befehl smo Clone Template abgeschlossen ist, ist die Klon-Spezifikations-Vorlage abgeschlossen.

```
smo clone template -profile SALES1 -backup-label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Verwandte Informationen

Erstellen von Klonspezifikationen

Klonen von Datenbanken aus Backups

Der Befehl smo Clone Update

Mit diesem Befehl werden Informationen zum Klon aktualisiert. Sie können den Kommentar aktualisieren.

Syntax

```
        smo clone update
-profile profile_name
\[-label label \| -id id\]
-comment  commment_text
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das den zu aktualisierenden Klon enthält. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-id**

  Gibt die ID für den Klon an. Die ID wird von SnapManager beim Erstellen eines Klons generiert. Verwenden Sie den Befehl smo Clone list, um die ID für jeden Klon anzuzeigen.

- * Label*

  Gibt die Bezeichnung für den Klon an.

- **-Kommentar**

  Zeigt den Kommentar an, der bei der Klonerstellung eingegeben wurde. Dies ist ein optionaler Parameter.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel wird der Klonkommentar aktualisiert.

```
smo clone update -profile anson.pcrac5
-label clone_pcrac51_20080820141624EDT -comment See updated clone
```

Der Befehl smo Clone Split-delete

Mit diesem Befehl können Sie einen Eintrag für den geteilten Klon-Vorgang aus einer Repository-Datenbank löschen.

Syntax

```
        smo clone split-delete
-profile profile \[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Profilnamen des Klons an.

- **-Host-Hostname**

  Gibt den Hostnamen an, in dem der Klon vorhanden ist.

- **-Label Split-Label**

  Gibt den Namen an, der durch den Prozess zum Starten des geteilten Klons generiert wurde.

- **-id Split-id**

  Gibt die eindeutige ID an, die durch den Prozess zum Starten des geteilten Klons generiert wird.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Der Befehl smo Clone Split-Schätzen

Mit diesem Befehl können Sie die abgeteilte Menge des für den Klon belegten Speicherplatzes anzeigen.

Syntax

```
        smo clone split-estimate
-profile profile
\[-host hostname\]
\[-label clone-label | -id clone-id\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Profilnamen des Klons an.

- **-Host-Hostname**

  Gibt den Hostnamen an, in dem der Klon vorhanden ist.

- **-Label Clone-Label**

  Gibt den durch den Klonprozess generierten Namen an.

- **-id Clone-id**

  Gibt die eindeutige ID an, die durch den Klonprozess generiert wurde.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Der Befehl smo Clone Split

Sie können den Befehl Clone Split ausführen, um einen Klon aufzuteilen. Der Split-Klon ist unabhängig vom ursprünglichen Klon. SnapManager generiert nach der Teilung des Klons ein neues Profil, und Sie können dieses Profil zum Verwalten des Split-Klons verwenden.

Syntax

```
        smo clone split
-profile clone-profile
\[-host hostname\]
\{-label clone-label | -id clone-id\} \[-split-label split-
operation_label\]
\[-comment comment\]
-new-profile new-profile-name \[-profile-password new-profile_password\]
-repository -dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database -dbname db_dbname
-host db_host \[-sid db_sid\] \[-login -username db_username -password
db_password
-port db_port\]
\[-rman \{\{-controlfile \| \{-login -username rman_username
-password rman_password\} -tnsname rman_tnsname\}\}\]
-osaccount osaccount
-osgroup osgroup
\[-retain
\[-hourly \[-count n\] \[-duration  m\]\]
\[-daily \[-count n\] \[-duration m\]\]
\[-weekly  \[-count n\] \[-duration m\]\]
\[-monthly \[-count n\] \[-duration m\]\] \]
\[-profile-comment profile-comment\]
\[-snapname-pattern pattern\]
\[-protect \[-protection-policy policy_name\]\] \| \[-noprotect\]\]
\[-summary-notification
\[-notification
\[-success -email email_address1,email_address2
-subject subject-pattern\]
\[failure -email email_address1,email_address2
-subject subject-pattern\] \]
[-separate-archivelog-backups
-retain-archivelog-backups
 -hours  hours |
-days days |
-weeks weeks |
-months months
[-protect \[-protection-policy policy_name \| -noprotect]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil Clone-Profil**

  Gibt den Profilnamen an, aus dem der Klon erstellt wird.

- **-Host-Hostname**

  Gibt den Host-Namen an, in dem der Klon vorhanden ist.

- **-Label Clone-Label**

  Gibt den vom Klonvorgang erzeugten Namen an.

- **-id Clone-id**

  Gibt die eindeutige ID an, die vom Klonvorgang generiert wird.

- **-Split-Label Split-Operation_Label**

  Gibt den vom Klonvorgang erzeugten Namen an.

- **-New-profile New-profile_Name**

  Gibt den neuen Profilnamen an, den SnapManager nach einem erfolgreichen Split-Vorgang generieren wird.

- **-profile-password New-profile_password**

  Gibt das Kennwort für das Profil an.

- **-Repository**

  Gibt die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem sich die Repository-Datenbank befindet.

- **-Port repo_Port**

  Gibt die TCP-Portnummer (Transmission Control Protocol) an, die für den Zugriff auf den Host verwendet wird, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an. Dies ist optional. Wenn nicht angegeben, verwendet SnapManager standardmäßig den Verbindungsmodus für OS-Authentifizierung.

- **-username repo_username**

Gibt den Benutzernamen an, der für den Zugriff auf den Host benötigt wird, auf dem sich die Repository-Datenbank befindet.

- **-Datenbank**

  Gibt die Details der Datenbank an, die gesichert, wiederhergestellt oder geklont werden soll.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem sich die Datenbank befindet.

- **-sid db_sid**

  Gibt die Systemkennung der Datenbank an, die das Profil beschreibt. Standardmäßig verwendet SnapManager den Datenbanknamen als Systemkennung. Falls sich die Systemkennung vom Datenbanknamen unterscheidet, müssen Sie sie mit der Option -sid angeben.

  Wenn Sie beispielsweise Oracle Real Application Clusters (RAC) verwenden, müssen Sie die Systemkennung der RAC-Instanz auf dem RAC-Knoten angeben, von dem aus SnapManager ausgeführt wird.

- **-Login**

  Gibt die Anmeldedaten für die Datenbank an.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-rman**

  Gibt die Details an, die SnapManager zum Katalogisieren von Backups mit dem Oracle Recovery Manager (RMAN) verwendet.

- **-controlfile**

  Gibt die Steuerdateien der Zieldatenbank als RMAN-Repository anstelle eines Katalogs an.

- **-Login**

  Gibt die RMAN-Anmeldedaten an.

- **-Passwort rman_password**

  Gibt das Kennwort an, mit dem Sie sich beim RMAN-Katalog anmelden können.

- **-username rman_Benutzername**

  Gibt den Benutzernamen an, der zum Anmelden beim RMAN-Katalog verwendet wird.

- **-tnsname tnsname**

  Gibt den Verbindungsnamen tnsname an (dieser wird in der Datei tsname.ora definiert).

- **-osaccount osconcount**

  Gibt den Namen des Benutzerkontos für die Oracle-Datenbank an. SnapManager verwendet dieses Konto, um die Oracle-Vorgänge wie dem Starten und Herunterfahren durchzuführen. Normalerweise ist es der Benutzer, der die Oracle-Software auf dem Host besitzt, zum Beispiel oracle.

- **-osgroup osgroup**

  Gibt den Namen der Oracle-Datenbankgruppe an, die dem oracle-Konto zugeordnet ist.

  Die Variablen -osaccount und -osgroup sind für UNIX erforderlich, jedoch nicht zulässig für Datenbanken, die unter Windows ausgeführt werden.

- **-halten [-hourly [-count n] [-duration m] [-taily [-count n] [-duration m]] [-Weekly [-count n] [-duration m]] [-monthly [-count n] [-duration m]]**

  Gibt die Aufbewahrungsrichtlinie für ein Backup an.

  Für jede Aufbewahrungsklasse kann entweder der Aufbewahrungszähler oder die Aufbewahrungsdauer angegeben werden. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). Wenn Sie beispielsweise nur eine Aufbewahrungsdauer von 7 für tägliche Backups angeben, wird SnapManager die Anzahl der täglichen Backups für das Profil nicht begrenzen (da die Aufbewahrungsanzahl 0 ist), aber SnapManager löscht automatisch tägliche Backups, die vor über 7 Tagen erstellt wurden.

- **-profile-comment Profil-comment**

  Gibt den Kommentar für ein Profil an, das die Profildomäne beschreibt.

- **-snapname-Muster**

  Gibt das Benennungsmuster für Snapshot Kopien an. Außerdem können Sie in allen Namen von Snapshot Kopien benutzerdefinierten Text einfügen, beispielsweise HAOPS für hochverfügbare Vorgänge. Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Snapshot Kopien, die vorhanden sind, behalten das vorherige SnapName-Muster bei. Sie können mehrere Variablen im Mustertext verwenden.

- **-protect -Protection-Policy_Name**

  Gibt an, ob das Backup auf dem sekundären Speicher gesichert werden soll.

  Wenn -protect ohne -Protection-Policy angegeben wird, dann hat der Datensatz keine Schutzpolitik. Wenn -protect angegeben wird und -Protection-Policy nicht gesetzt wird, wenn das Profil erstellt wird, dann kann es später durch den smo profile Update Befehl oder durch den Storage Administrator über die Protection Manager Konsole gesetzt werden.

- **-summary-notification**

  Gibt die Details zur Konfiguration einer E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank an. SnapManager generiert diese E-Mail.

- **-Benachrichtigung**

  Gibt die Details zur Konfiguration der E-Mail-Benachrichtigung für das neue Profil an. SnapManager generiert diese E-Mail. Die E-Mail-Benachrichtigung ermöglicht es dem Datenbankadministrator, E-Mails über den Status erfolgreich oder fehlgeschlagen des Datenbankvorgangs zu erhalten, der mit diesem Profil ausgeführt wird.

- **-Erfolg**

  Gibt an, dass die E-Mail-Benachrichtigung für ein Profil aktiviert ist, für das der SnapManager-Vorgang erfolgreich ist.

- **-email address 1 email address 2**

  Gibt die E-Mail-Adresse des Empfängers an.

- **-Betreff-Muster**

  Gibt den Betreff für die E-Mail an.

- **-Versagen**

  Gibt an, dass die E-Mail-Benachrichtigung für ein Profil aktiviert ist, für das der SnapManager-Vorgang fehlschlägt.

- **-separate-archivlog-Backups**

  Gibt an, dass die Backup des Archivprotokolls von der Datendatei-Sicherung getrennt ist. Dies ist ein optionaler Parameter, den Sie bei der Erstellung des Profils angeben können. Nachdem die Backups mit dieser Option getrennt wurden, können Sie entweder nur Datendateien Backup oder ausschließlich Archivprotokolle erstellen.

- **-behalten-archivelog-Backups -Stunden- -Tage- Wochen- Monthsmonths**

  Gibt an, dass die Archiv-Log-Backups auf Basis der Aufbewahrungsdauer des Archivprotokolls (stündlich, täglich, wöchentlich oder monatlich) aufbewahrt werden.

- **Schutz [-Schutz-policypolicy_Name] -noprotect**

  Gibt an, dass die Archivprotokolldateien auf der Grundlage der Archivierungsprotokollschutzrichtlinie geschützt sind.

  Gibt an, dass die Archivprotokolldateien nicht mit der Option -noprotect geschützt sind.

- **-enthalten-mit-online-Backups**

  Gibt an, dass das Backup des Archivprotokolls zusammen mit dem Online-Datenbank-Backup enthalten ist.

  Gibt an, dass die Archiv-Log-Backups nicht zusammen mit dem Online-Datenbank-Backup enthalten sind.

- **-dump**

  Gibt an, dass die Dump-Dateien nach dem erfolgreichen Erstellen des Profils nicht erfasst werden.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Die Standardeinstellung zeigt Fehler- und Warnmeldungen an.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Der Befehl smo Clone Split-Ergebnis

Syntax

Mit diesem Befehl können Sie das Ergebnis des Klon-Split-Prozesses anzeigen.

```
        smo clone split-result
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Profilnamen des Klons an.

- **-Host-Hostname**

  Gibt den Hostnamen an, in dem der Klon vorhanden ist.

- **-Label Split-Label**

  Gibt den Namen an, der durch den Prozess zum Starten des geteilten Klons generiert wurde.

- **-id Split-id**

  Gibt eine eindeutige ID an, die durch den Prozess zum Starten des geteilten Klons generiert wurde.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Der Befehl smo Clone Split-stop

Mit diesem Befehl wird der Splittprozess für den ausgeführten Klon angehalten.

Syntax

```
        smo clone split-stop
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Profilnamen des Klons an.

- **-Host-Hostname**

  Gibt den Hostnamen an, in dem der Klon vorhanden ist.

- **-Label Split-Label**

  Gibt den durch den Klonprozess generierten Namen an.

- **-id Split-id**

  Gibt die eindeutige ID an, die durch den Klonprozess generiert wurde.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Der Befehl smo Clone Split-Status

Mit diesem Befehl können Sie den Fortschritt der Ausführung des Split-Prozesses kennen.

Syntax

```
        smo clone split-status
-profile profile
\[-host hostname\]
\[-label split-label \| -id split-id\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Profilnamen des Klons an.

- **-Host-Hostname**

  Gibt den Hostnamen an, in dem der Klon vorhanden ist.

- **-Label Split-Label**

  Gibt den durch den Klonprozess generierten Namen an.

- **-id Split-id**

  Gibt die eindeutige ID an, die durch den Klonprozess generiert wurde.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Der Befehl Smo Clone Trennen

Nach dem Aufteilen eines geklonten Volumes aus seinem übergeordneten Volume in Data ONTAP können Sie den Befehl „Clone Trennen“ (Abtrennen) von SnapManager ausführen und SnapManager darauf informieren, dass es sich bei dem Volume nicht mehr um einen Klon handelt.

Syntax

smo Clone Trennen -profile_Name -Label Clone_Label

Parameter

- **-profile Profile_Name**

  Gibt den Profilnamen an, aus dem der Klon erstellt wird.

- **-Label Clone_Label**

Gibt den Namen an, der vom Klonvorgang generiert wurde.

Beispiel

Mit dem folgenden Befehl wird der Klon enttrennt:

```
smo clone detach -profile SALES1 -label sales1_clone
```

Der Befehl smo cmdfile

Sie können den Befehl cmdfile verwenden, um jeden beliebigen Befehl auszuführen, wenn die Shell auf Ihrem Host die Anzahl der Zeichen begrenzt, die in einer Befehlszeile angezeigt werden können.

Syntax

```
        smo cmdfile
-file file_name
\[-quiet \| -verbose\]
```

Sie können den Befehl in eine Textdatei einfügen und den Befehl smo cmdfile verwenden, um den Befehl auszuführen. Sie können nur einen Befehl in einer Textdatei hinzufügen. Sie dürfen smo nicht in die Befehlssyntax einschließen.

Der Befehl smo cmdfile ersetzt den Befehl smo pfile. Die smo cmdfile ist nicht mit dem Befehl smo pfile kompatibel.

Parameter

- **-file file_Name**

  Gibt den Pfad zur Textdatei an, die den Befehl enthält, den Sie ausführen möchten.

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen in der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen in der Konsole angezeigt werden.

Beispiel

Dieses Beispiel erstellt ein Profil, indem der Befehl Profile create in command.txt unter /tmp eingeschlossen wird. Sie können dann den Befehl smo cmdfile ausführen.

Die Textdatei enthält folgende Informationen:

```
profile create -profile SALES1 -repository -dbname SNAPMGRR
-login -username server1_user -password ontap -port 1521 -host server1
-database -dbname SMO -sid SMO -login -username sys -password oracle -port
1521
-host Host2 -osaccount oracle -osgroup db2
```

Sie können das Profil jetzt erstellen, indem Sie den Befehl smo cmdfile mit der Datei command.txt ausführen:

```
smo cmdfile -file /tmp/command.txt
```

Der Befehl smo Credential Clear

Mit diesem Befehl wird der Cache der Benutzeranmeldeinformationen für alle gesicherten Ressourcen gelöscht.

Syntax

```
        smo credential clear
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

In diesem Beispiel werden alle Anmeldeinformationen für den Benutzer gelöscht, der den Befehl ausführt.

```
smo credential clear -verbose
```

```
SMO-20024 [INFO ]: Cleared credentials for user "user1".
```

Verwandte Informationen

Löschen von Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile

Der Befehl zum Löschen von Smo-Anmeldeinformationen

Mit diesem Befehl werden die Benutzeranmeldeinformationen für eine bestimmte gesicherte Ressource gelöscht.

Syntax

```
        smo credential delete
\[-host -name host_name
-username username\] \|
[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port\] \|
\[-profile
-name profile_name\]
[-quiet | -verbose]
```

Parameter

- **-Host-Hostname**

  Gibt den Namen des Host-Servers an, auf dem SnapManager ausgeführt wird.

  Der Parameter -Host enthält die folgenden Optionen:

  - -Name Host_Name: Gibt den Namen des Hosts an, für den Sie das Passwort löschen möchten.
  - -Username user_Name: Gibt den Benutzernamen auf dem Host an.
- **-Repository -dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

  Der Parameter -Repository enthält die folgenden Optionen:

  - -Dbnamerepo_Service_Name: Gibt den Namen der Datenbank an, die das Profil speichert. Verwenden Sie entweder den globalen Namen oder den SID.
  - -Host repo_Host: Gibt den Namen oder die IP-Adresse des Hostservers an, auf dem die Repository-Datenbank ausgeführt wird.
  - -Login-username repo_username: Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.
  - -Port repo_Port: Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.
- **-profile -Name profile_Name**

  Gibt das Profil an, mit dem die Datenbank verknüpft ist.

Der Parameter -profile enthält die folgende Option:

- -Name profilname: Gibt den Namen des Profils an, für das Sie das Passwort löschen werden.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

In diesem Beispiel werden die Anmeldeinformationen des Profils gelöscht.

```
smo credential delete -profile -name user1 -verbose
```

```
SMO-20022 [INFO ]: Deleted credentials and repository mapping
 for profile "user1" in user credentials for "user1".
```

In diesem Beispiel werden die Anmeldeinformationen des Repositorys gelöscht.

```
smo credential delete -repository -dbname SMOREPO -host Host2
-login -username user1 -port 1521
```

```
SMO-20023 [INFO ]: Deleted repository credentials for
"user1@SMOREPO/wasp:1521"
and associated profile mappings in user credentials for "user1".
```

In diesem Beispiel werden die Anmeldeinformationen des Hosts gelöscht.

```
smo credential delete -host -name Host2
```

```
SMO-20033 [INFO ]: Deleted host credentials for "Host2" in user
credentials for "user1".
```

Verwandte Informationen

Löschen von Anmeldeinformationen für einzelne Ressourcen

Der Befehl smo Anmeldeinformationsliste

Dieser Befehl listet alle Anmeldedaten eines Benutzers auf.

Syntax

```
        smo credential list
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

In diesem Beispiel werden alle Anmeldeinformationen für den Benutzer angezeigt, der den Befehl ausführt.

```
smo credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMOREPO/hotspur:1521
Host2_test_user@SMOREPO/hotspur:1521
user1_1@SMOREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]
Hosts:
Host2
Host5
Host4
Host1
```

Verwandte Informationen

Anzeigen von Benutzeranmeldeinformationen

Der Befehl Smo Credential Set

Mit diesem Befehl können Sie die Anmeldeinformationen für Benutzer festlegen, die auf sichere Ressourcen wie Hosts, Repositorys und Datenbankprofile zugreifen können. Das Host-Passwort ist das Passwort des Benutzers auf dem Host, auf dem SnapManager ausgeführt wird. Das Repository-Kennwort ist das Kennwort des Oracle-Benutzers, der das SnapManager-Repository-Schema enthält. Das Profilkennwort ist ein Passwort, das von der Person, die das Profil erstellt, gebildet wird. Wenn bei den Host- und Repository-Optionen die Option optional -password nicht enthalten ist, werden Sie aufgefordert, ein Kennwort des in den Befehlsargumenten angegebenen Typs einzugeben.

Syntax

```
        smo credential set
\[-host
-name host_name
-username username\]
\[-password password\] \] \|
\[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username\] \[-password repo_password\] \]
-port repo_port \|
\[-profile
-name profile_name\]
\[-password password\] \]
\[-quiet \| -verbose\]
```

Parameter

- **-Host-Hostname**

  Gibt den Namen oder die IP-Adresse des Hostservers an, auf dem SnapManager ausgeführt wird.

  Der Parameter -Host enthält die folgenden Optionen:

  - -Name Host_Name: Gibt den Namen des Hosts an, für den Sie das Passwort festlegen möchten.
  - -Username user_Name: Gibt den Benutzernamen auf dem Host an.
  - -Password password: Gibt das Passwort des Benutzers auf dem Host an.

- **-Repository -dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

  Der Parameter -Repository enthält die folgenden Optionen:

  - -Dbnamerepo_Service_Name: Gibt den Namen der Datenbank an, die das Profil speichert. Verwenden

Sie entweder den globalen Namen oder den SID.

- -Host repo_Host: Gibt den Namen oder die IP-Adresse des Hostservers an, auf dem die Repository-Datenbank ausgeführt wird.
- -Login-username repo_username: Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.
- -Password password: Gibt das Kennwort an, das für den Zugriff auf die Datenbank, die das Repository speichert, erforderlich ist.
- -Port repo_Port: Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-profile -Name profile_Name**

  Gibt das Profil an, mit dem die Datenbank verknüpft ist.

  Der Parameter -profile enthält die folgende Option:

  - -Name profilname: Gibt den Namen des Profils an, für das Sie das Passwort festlegen.
  - -Password password: Gibt das Passwort an, das für den Zugriff auf das Profil erforderlich ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl zum Festlegen von Repository-Anmeldedaten

Im folgenden Beispiel werden Anmeldeinformationen für ein Repository festgelegt.

```
smo credential set -repository -dbname SMOREPO -host hotspur -port 1521
-login -username chris
Password for chris@hotspur:1521/SMOREPO : ********
Confirm password for chris@hotspur:1521/SMOREPO : ********
```

```
SMO-12345 [INFO ]: Updating credential cache for OS user "admin1"
SMO-12345 [INFO ]: Set repository credential for user "user1" on
repo1@Host2.
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

Beispiel-Befehl zum Festlegen von Host-Anmeldedaten

Da eine Hostanmeldeinformationen eine tatsächliche Betriebssystemanmeldeinformationen darstellen, muss sie zusätzlich zum Passwort den Benutzernamen enthalten.

```
smo credential set -host -name bismarck -username avida
Password for avida@bismarck : ********
Confirm password for avida@bismarck : ********
```

Verwandte Informationen

Wie SnapManager die Sicherheit gewährleistet

Der Befehl smo history list

Mit diesem Befehl können Sie eine Liste der Verlaufsdetails für den SnapManager-Vorgang anzeigen.

Syntax

```
        smo history list
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank

ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

  Gibt den SnapManager-Vorgang an, für den Sie den Verlauf konfigurieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history list -profile -name PROFILE1 -operation -operations
backup -verbose
```

Der Befehl smo history Operation-show

Mit diesem Befehl können Sie den Verlauf eines bestimmten SnapManager-Vorgangs, der einem Profil zugeordnet ist, anzeigen.

Syntax

```
        smo history operation-show
-profile profile
\{-label label \| -id id\}
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- * Label-Label. -idid*

  Gibt die SnapManager-Vorgangs-ID oder -Bezeichnung an, für die Sie den Verlauf anzeigen möchten.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history operation-show -profile PROFILE1 -label backup1
-verbose
```

Der Befehl Smo history purge

Mit diesem Befehl können Sie den Verlauf des SnapManager-Vorgangs löschen.

Syntax

```
        smo history purge
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

  Gibt den SnapManager-Vorgang an, für den Sie den Verlauf konfigurieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

Der Befehl smo history remove

Mit diesem Befehl können Sie den Verlauf der SnapManager-Vorgänge entfernen, die mit einem einzelnen Profil, mehreren Profilen oder allen Profilen in einem Repository verknüpft sind.

Syntax

```
        smo history remove
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name,
operation_name2\] \| -all\}
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

Gibt den SnapManager-Vorgang an, für den Sie den Verlauf konfigurieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

Der Befehl smo history set

Sie können den Befehl History Set ausführen, um die Vorgänge zu konfigurieren, für die Sie den Verlauf anzeigen möchten.

Syntax

```
        smo history set
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
-retain
{-count retain_count \| -daily daily_count \| -monthly monthly_count \|
-weekly weekly_count}
[-quiet | -verbose]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Der Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

Gibt die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hosts an, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Port repo_Port**

  Gibt die Portnummer des Transmission Control Protocol (TCP) an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

  Gibt die SnapManager Vorgänge an, für die Sie den Verlauf konfigurieren möchten.

- **-contain {-countretain_count -dailytaily_count}**

  Gibt die Aufbewahrungsklasse der Backup-Erstellung an, prüft Backup, Wiederherstellung und Wiederherstellung und erstellt und aufgeteilt von Klonvorgängen. Die Aufbewahrungsklasse wird basierend auf der Anzahl der Vorgänge, der Anzahl der Tage, Wochen oder Monate festgelegt.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden Informationen zum Sicherungsvorgang angezeigt:

```
smo history set -profile -name PROFILE1 -operation -operations backup
-retain -daily 6
 -verbose
```

Der Befehl smo history show

Mit diesem Befehl können Sie detaillierte Verlaufsinformationen für ein bestimmtes Profil anzeigen.

Syntax

```
        smo history show
-profile profile
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history show -profile -name PROFILE1
 -verbose
```

Der Befehl smo help

Sie können den Hilfe-Befehl ausführen, um Informationen zu den SnapManager-Befehlen und ihren Optionen anzuzeigen. Wenn Sie keinen Befehlsnamen angeben, wird eine Liste der gültigen Befehle angezeigt. Wenn Sie einen Befehlsnamen angeben, wird die Syntax für den Befehl angezeigt.

Syntax

```
        smo help
\[backup\|cmdfile\|clone\|credential\|help\|operation\|profile\|protection
-policy\|repository\|system\|version\|plugin\|diag\|history\|schedule\|not
ification\|storage\|get\]
\[-quiet \| -verbose\]
```

Parameter

Im Folgenden sind einige Befehlsnamen, die Sie mit diesem Befehl verwenden können:

- Backup
- Klon
- Cmdfile
- Anmeldedaten
- diag
- Get
- Benachrichtigung
- Hilfe
- Verlauf
- Betrieb
- Plug-in
- Profil
- Sicherungsrichtlinie
- Repository
- Zeitplan
- Storage
- System
- Version

Der Befehl smo notification remove-summary-notification

Mit diesem Befehl wird die Überblickbenachrichtigung für mehrere Profile in einer Repository-Datenbank deaktiviert.

Syntax

```
        smo notification remove-summary-notification
-repository
-dbname repo_service_name
-port repo_port
-host repo_host
-login -username repo_username
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login repo_username**

  Gibt den Anmeldenamen an, der für den Zugriff auf die Datenbank, in der das Repository gespeichert ist, erforderlich ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Im folgenden Beispiel wird die Überblickbenachrichtigung für mehrere Profile in einer Repository-Datenbank deaktiviert.

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login -username oba5
```

Der Befehl smo notification Update-summary-notification

Sie können den Befehl Notification Update-summary-notification ausführen, um eine zusammenfassende Benachrichtigung für eine Repository-Datenbank zu aktivieren.

Syntax

```
        smo notification update-summary-notification
-repository
-port repo_port
-dbname  repo_service_name
-host repo_host
-login -username repo_username
-email email-address1,email-address2
-subject subject-pattern
-frequency
[-daily –time daily_time \|
-hourly –time hourly_time \|
-monthly –time monthly_time -date \[1\|2\|3\|...\|31\] \|
-weekly  –time weekly_time -day \[1\|2\|3\|4\|5\|6\|7\]\]
-profiles profile1,profile2
-notification-host notification-host
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Gibt die Details der Repository-Datenbank an.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- **-dbname repo_Service_Name**

  Gibt den Namen der Repository-Datenbank an. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hosts an, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an. Dies ist optional. Wenn nicht angegeben, verwendet SnapManager standardmäßig den Verbindungsmodus für OS-Authentifizierung.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Email-Adresse1, E-Mail-Adresse2**

  Gibt E-Mail-Adressen der Empfänger an.

- **-Betreff-Muster**

Gibt das Muster für E-Mail-Betreff an.

- **-Frequenz { -täglich --Zeit Tageszeit - stündlich --Zeit Stundenweise --Zeit monatlich --Zeit monatlich_Zeit -Datum {1 natürlich 3… 31 } --Zeit wöchentlich - Zeit wöchentlich - Tag {1 2 3 4 5 natürlich 6 7 } }**

  Gibt den Terminplantyp und die Zeitplandauer an, wann die E-Mail-Benachrichtigung angezeigt werden soll.

- **-Profile profil1, profil2**

  Gibt Profilnamen an, die E-Mail-Benachrichtigungen erfordern.

- **-notification-Host notification-Host**

  Gibt den SnapManager-Server-Host an, von dem aus die Zusammenfassung Benachrichtigungs-E-Mail an die Empfänger gesendet wird. Sie können Hostnamen oder IP-Adressen für den Benachrichtigungs-Host angeben. Sie können auch die Host-IP oder den Host-Namen aktualisieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Das folgende Beispiel ermöglicht eine zusammenfassende Benachrichtigung für eine Repository-Datenbank:

```
smo notification update-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5 –email
admin@org.com –subject success –frequency -daily -time 19:30:45 –profiles
sales1
```

Der Befehl smo notification set

Sie können den E-Mail-Server mit dem Befehl Notification Set konfigurieren.

Syntax

```
        smo notification set
-sender-email email_address
-mailhost mailhost
-mailport mailport
[-authentication
-username username
-password password]
-repository
-dbname repo_service_name
-port repo_port]
-host repo_host
-login -username repo_username
[-quiet | -verbose]
```

Parameter

- **-Absender-Email_address**

  Gibt die E-Mail-Adresse des Absenders an, von der die E-Mail-Benachrichtigungen gesendet werden. Ab SnapManager 3.2 für Oracle können Sie einen Bindestrich (-) einfügen, während Sie den Domain-Namen der E-Mail-Adresse angeben. Sie können beispielsweise die Absender-E-Mail-Adresse als -sender-email07lbfmdatacenter@continental-corporation.com angeben.

- **-mailhost mailhost**

  Gibt den Namen oder die IP-Adresse des Hostservers an, der E-Mail-Benachrichtigungen verarbeitet.

- **-mailport mailport**

  Gibt die Portnummer des Mail-Servers an.

- **-Authentifizierung -Benutzername -Passwort-Passwort**

  Gibt Authentifizierungsdetails für die E-Mail-Adresse an. Sie müssen Benutzernamen und Passwort angeben.

- **-Repository**

  Gibt die Details der Repository-Datenbank an.

- **-Port repo_Port**

  Gibt die Portnummer des Transmission Control Protocol (TCP) an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- **-dbname repo_Service_Name**

  Gibt den Namen der Repository-Datenbank an. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

Gibt den Namen oder die IP-Adresse des Hosts an, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an. Dies ist optional. Wenn nicht angegeben, verwendet SnapManager standardmäßig den Verbindungsmodus für OS-Authentifizierung.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird der Mail-Server konfiguriert:

```
smo notification set -sender-email admin@org.com -mailhost
hostname.org.com -mailport 25 authentication -username davis -password
davis -repository -port 1521 -dbname SMOREPO -host hotspur
-login -username grabal21 -verbose
```

Der Befehl Smo Operation Dump

Sie können den Befehl Operation Dump ausführen, um eine JAR-Datei zu erstellen, die Diagnoseinformationen zu einem Vorgang enthält.

Syntax

```
        smo operation dump
-profile profile_name
\[-label label_name \| -id guid\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie die Speicherauszugsdateien erstellen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Label Label Label_Name**

Erstellt Dump-Dateien für den Vorgang und weist die angegebene Bezeichnung zu.

- **-id-Guid**

  Erstellt Dump-Dateien für den Vorgang mit der angegebenen GUID. Die GUID wird von SnapManager generiert, wenn der Vorgang beginnt.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird die Dump-Datei für das Backup erstellt:

```
smo operation dump -profile SALES1
-id 8abc01ec0e78f3e2010e78f3fdd00001
```

```
Dump file created
Path:/userhomedirectory/.netapp/smo/3.3/smo_dump_8abc01ec0e78f3e2010e78f3f
dd00001.jar
```

Verwandte Informationen

Speicherauszug-Dateien

Befehl smo Operation list

Mit diesem Befehl werden die Zusammenfassungsinformationen aller Vorgänge aufgelistet, die für ein bestimmtes Profil aufgezeichnet wurden.

Syntax

```
        smo operation list
-profile profile_name
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Trennzeichen**

  (Optional) Wenn dieser Parameter angegeben wird, listet der Befehl jede Zeile in einer separaten Zeile auf und die Attribute in dieser Zeile werden durch das angegebene Zeichen getrennt.

- **-ruhig**

  (Optional) zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  (Optional) zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden die Zusammenfassungsinformationen aller Vorgänge aufgeführt, die mit dem angegebenen Profil protokolliert wurden.

```
smo operation list -profile myprofile
```

```
Start Date Status Operation ID Type Host
-------------------- ---------- --------------------------------
------------------ --
2007-07-16 16:03:57 SUCCESS 8abc01c813d0a1530113d0a15c5f0005 Profile
Create Host3
2007-07-16 16:04:55 FAILED 8abc01c813d0a2370113d0a241230001 Backup Host3
2007-07-16 16:50:56 SUCCESS 8abc01c813d0cc580113d0cc60ad0001 Profile
Update Host3
2007-07-30 15:44:30 SUCCESS 8abc01c81418a88e011418a8973e0001 Remove Backup
Host3
2007-08-10 14:31:27 SUCCESS 8abc01c814510ba20114510bac320001 Backup Host3
2007-08-10 14:34:43 SUCCESS 8abc01c814510e9f0114510ea98f0001 Mount Host3
2007-08-10 14:51:59 SUCCESS 8abc01c814511e6e0114511e78d40001 Unmount Host3
```

Verwandte Informationen

Anzeigen einer Liste von Vorgängen

Der Befehl smo Operation show

Sie können den Befehl „Operation show“ ausführen, um die Zusammenfassungsinformationen aller Vorgänge, die für das angegebene Profil durchgeführt wurden, aufzulisten. Die Ausgabe listet den Client-Benutzer (den Benutzer für den Client-PC) und den effektiven Benutzer (den Benutzer in SnapManager, der auf

dem ausgewählten Host gültig ist) auf.

Syntax

```
        smo operation show
-profile profile_name
\[-label label \| -id id\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- * Label*

  Gibt die Bezeichnung für den Vorgang an.

- **-id-id**

  Gibt die Kennung für den Vorgang an.

- **-ruhig**

  Optional: Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Optional: Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

In der folgenden Befehlszeile werden detaillierte Informationen über einen Vorgang angezeigt:

```
# smo operation show -profile myprofile -id
ff8080811295eb1c011295eb28230001
```

```
Operation Attempted
   Operation ID: ff8080811295eb1c011295eb28230001
   Type:RestoreFor profile: myprofile
   With Force: No
   Performed on backup
   Operation ID: ff8080811295eb1c011296eb23290001
   Label: mylabel
Operation Runtime Information
   Status: SUCCESS
   Start date: 2007-07-16 13:24:09 IST
   End date: 2007-07-16 14:10:10 IST
   Client user: amorrow
   Effective user: amorrow
Host
   Host Run upon: Host3
   Process ID: 3122
   SnapManager version: 3.3
Repository
   Connection: user1@SMOREPO/hotspur:1521
   Repository version: 3.3
Resources in use
   Volume:
     ssys1:/vol/luke_ES0_0 (FlexClone)
   Filesystems:
     /opt/NetApp/smo/mnt/-
mnt_ssys1_luke_ES0_smo_e_es0_f_c_1_8abc0112129b0f81580001_0
```

Verwandte Informationen

Anzeigen von Betriebsdetails

Der Befehl smo password Reset

Sie können den Befehl zum Zurücksetzen des Passworts ein Profil zurücksetzen.

Syntax

```
        smo password reset
-profile profile
\[-profile-password profile_password\]
\[-repository-hostadmin-password repository_hostadmin_password\]
[-quiet | -verbose]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an, für das Sie das Passwort zurücksetzen möchten.

- **-profile-password Profil_password**

  Gibt das neue Kennwort für das Profil an.

- **-Repository-hostadmin-password admin_password**

  Gibt die autorisierten Benutzerberechtigungen mit Root-Berechtigung für die Repository-Datenbank an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Der smo Plugin Check Befehl

SnapManager ermöglicht Ihnen die Installation und Verwendung benutzerdefinierter Skripte für verschiedene Vorgänge. SnapManager bietet Backup, Restore und Klon-Plug-ins, um Ihre individuellen Skripte vor und nach Backup-, Restore- und Klonvorgängen zu automatisieren. Bevor Sie das Backup-, Wiederherstellungs- und Klon-Plug-in verwenden, können Sie den Plugin Check-Befehl ausführen, um die Installation von Plug-in-Skripten zu überprüfen. Benutzerdefinierte Skripts werden in drei Verzeichnissen gespeichert: Richtlinie (für Skripte, die immer vor Backup-, Wiederherstellungs- oder Klonvorgang ausgeführt werden sollten), vor (für Vorverarbeitungsskripte) und Post (für Skripte bei der Nachbearbeitung).

Syntax

```
        smo plugin check

-osaccount os_db_user_name
```

Parameter

- **-osconter**

  Gibt den Benutzernamen für die Betriebssystemdatenbank an. Wenn Sie die Option -oskonto nicht eingeben, prüft SnapManager die Plug-in-Skripte als Root-Benutzer und nicht als bestimmten Benutzer.

Beispiel

Das folgende Beispiel zeigt, dass der Befehl Plugin Check das benutzerdefinierte Skript Policy 1 gefunden hat, das im Verzeichnis Policy als ausführbare Datei gespeichert ist. Das Beispiel zeigt auch, dass die beiden anderen im Vorverzeichnis gespeicherten benutzerdefinierten Skripte keine Fehlermeldungen ausgeben (angezeigt mit dem Status 0); das vierte benutzerdefinierte Skript (Post-Plug-in1), das im Post-Verzeichnis gefunden wurde, enthält jedoch Fehler (angezeigt mit dem Status 3).

```
smo plugin check
Checking plugin directory structure ...
<installdir>/plugins/clone/policy
OK: 'policy1' is executable
<installdir>/plugins/clone/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/clone/post
ERROR: 'post-plugin1' is executable and returned status 3
<installdir>/plugins/backup/policy
OK: 'policy1' is executable
<installdir>/plugins/backup/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/backup/post
ERROR: 'post-plugin1' is executable and returned status 3
<installdir>/plugins/restore/policy
OK: 'policy1' is executable
<installdir>/plugins/restore/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/restore/post
ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

Verwandte Informationen

Klonen von Datenbanken und mit benutzerdefinierten Plug-in-Skripten

Der Befehl smo profile create

Sie können den Befehl Profile create ausführen, um ein Profil einer Datenbank in einem Repository zu erstellen. Sie müssen die Datenbank mounten, bevor Sie diesen Befehl ausführen.

Syntax

```
        smo profile create
-profile profile
```

```
\[-profile-password profile_password\]
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database
-dbname db_dbname
-host db_host
[-sid  db_sid\]
[-login
\[-username db_username -password db_password -port db_port\]
 \[-asminstance -asmusername asminstance_username  -asmpassword
asminstance_password\]]
[-rman \{-controlfile \| \{-login
-username  rman_username -password  rman_password\}
-tnsname  rman_tnsname\}\}]
\[-osaccount osaccount \]
\[-osgroup osgroup\]
[-retain
\[-hourly \[-count n\] \[-duration m\]\]
\[-daily \[-count n\] \[-duration m\]]
\[-weekly \[-count n\] \[-duration m\]]
\[-monthly \[-count n\] \[-duration m\]]]]
-comment comment
-snapname-pattern pattern
[-protect \[-protection-policy policy\]]
[-summary-notification]
[-notification
\[-success
-email email_address1,email_address2
-subject subject_pattern\]
\[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups
-retain-archivelog-backups
 -hours hours |
-days days |
-weeks weeks |
-months months
[-protect \[-protection-policy policy_name \| -noprotect]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
[-quiet | -verbose]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-profile-password Profil_password**

  Geben Sie das Kennwort für das Profil an.

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-sid db_sid**

  Gibt die Systemkennung der Datenbank an, die das Profil beschreibt. Standardmäßig verwendet SnapManager den Datenbanknamen als Systemkennung. Falls sich die Systemkennung vom Datenbanknamen unterscheidet, müssen Sie sie mit der Option -sid angeben.

  Wenn Sie beispielsweise Oracle Real Application Clusters (RAC) verwenden, müssen Sie die Systemkennung der RAC-Instanz auf dem RAC-Knoten angeben, von dem aus SnapManager ausgeführt wird.

- **-Login**

  Gibt die Anmeldedaten für das Repository an.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- **-Datenbank**

  Gibt die Details der Datenbank an, die das Profil beschreibt. Diese Datenbank wird gesichert, wiederhergestellt und geklont.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen

oder die Systemkennung verwenden.

- **-Host db_Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Datenbank ausgeführt wird.

- **-asminstance**

  Gibt die Anmeldeinformationen an, die zur Anmeldung bei der Instanz für die automatische Speicherverwaltung (ASM) verwendet werden.

- **-asmusername asminstance_username**

  Gibt den Benutzernamen an, der zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-asmpassword asminstance_password**

  Gibt das Kennwort an, das zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-Login**

  Gibt die Anmeldedaten für die Datenbank an.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Port db_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, die das Profil beschreibt.

- **-rman**

  Gibt die Details an, die SnapManager zum Katalogisieren von Backups mit dem Oracle Recovery Manager (RMAN) verwendet.

- **-controlfile**

  Gibt die Steuerdateien für die Zieldatenbank an, anstatt einen Katalog als RMAN-Repository zu verwenden.

- **-Login**

  Gibt die RMAN-Anmeldedaten an.

- **-Passwort rman_password**

  Gibt das Kennwort an, mit dem Sie sich beim RMAN-Katalog anmelden können.

- **-username rman_Benutzername**

Gibt den Benutzernamen an, der zum Anmelden beim RMAN-Katalog verwendet wird.

- **-tnsname tnsname**

  Gibt den Verbindungsnamen tnsname an (dieser wird in der Datei tsname.ora definiert).

- **-osaccount osconcount**

  Gibt den Namen des Benutzerkontos für die Oracle-Datenbank an. SnapManager verwendet dieses Konto, um die Oracle-Vorgänge wie dem Starten und Herunterfahren durchzuführen. Normalerweise ist es der Benutzer, der die Oracle-Software auf dem Host besitzt, zum Beispiel oracle.

- **-osgroup osgroup**

  Gibt den Namen der Oracle-Datenbankgruppe an, die dem oracle-Konto zugeordnet ist.

- **-halten [-hourly [-count n] [-duration m] [-taily [-count n] [-duration m]] [-Weekly [-count n] [-duration m]] [-monthly [-count n] [-duration m]]**

  Gibt die Aufbewahrungsrichtlinie für ein Backup an, bei dem entweder oder beide Aufbewahrungsdaten zusammen mit einer Aufbewahrungsdauer für eine Aufbewahrungsklasse (stündlich, täglich, wöchentlich, monatlich) zählen.

  Für jede Aufbewahrungsklasse kann entweder oder beides einer Anzahl von Aufbewahrungsfristen oder eine Aufbewahrungsdauer angegeben werden. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). Wenn der Benutzer beispielsweise nur eine Aufbewahrungsdauer von 7 für tägliche Backups angibt, dann wird SnapManager nicht die Anzahl der täglichen Backups für das Profil begrenzen (da die Aufbewahrungsanzahl 0 ist), aber SnapManager löscht automatisch täglich erstellte Backups, die vor 7 Tagen erstellt wurden.

- **-Kommentar**

  Gibt den Kommentar für ein Profil an, das die Profildomäne beschreibt.

- **-snapname-Muster**

  Gibt das Benennungsmuster für Snapshot Kopien an. Außerdem können Sie in allen Namen von Snapshot Kopien benutzerdefinierten Text einfügen, beispielsweise HAOPS für hochverfügbare Vorgänge. Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Snapshot Kopien, die vorhanden sind, behalten das vorherige SnapName-Muster bei. Sie können mehrere Variablen im Mustertext verwenden.

- **-protect -Protection-Policy**

  Gibt an, ob das Backup auf sekundärem Storage gesichert werden soll.

  > Wenn -protectis ohne -Protection-Policy angegeben wird, dann hat der Datensatz keine Schutzrichtlinie. Wenn -protect angegeben wird und -Protection-Policy beim Erstellen des Profils nicht festgelegt wird, kann es später einen Befehl zur Aktualisierung von Bysmo-Profilen geben oder vom Speicheradministrator über die Konsole von Protection Manager festgelegt werden.

- **-summary-notification**

Gibt an, dass die E-Mail-Benachrichtigung für das neue Profil aktiviert ist.

- **-notification -success-email e-Mail_adress1,E-Mail address2 -subject_pattern**

  Gibt an, dass die E-Mail-Benachrichtigung für das neue Profil aktiviert ist, so dass E-Mails von Empfängern empfangen werden, wenn der SnapManager-Vorgang erfolgreich ist. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den E-Mail-Betreff für das neue Profil.

  Sie können auch benutzerdefinierten Subjekttext für das neue Profil einfügen. Sie können den Betreff ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-notification -Failure -Email-Mail_adress1,E-Mail address2 -subject_pattern**

  Gibt an, dass die E-Mail-Benachrichtigung aktivieren für das neue Profil aktiviert ist, damit E-Mails von Empfängern empfangen werden, wenn der SnapManager-Vorgang fehlschlägt. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den E-Mail-Betreff für das neue Profil.

  Sie können auch benutzerdefinierten Subjekttext für das neue Profil einfügen. Sie können den Betreff ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-separate-archivlog-Backups**

  Gibt an, dass die Backup des Archivprotokolls von der Datendatei-Sicherung getrennt ist. Dies ist ein optionaler Parameter, den Sie beim Erstellen des Profils angeben können. Nachdem Sie die Sicherung mit dieser Option getrennt haben, können Sie entweder Datendateien-only-Backup oder Archiv-Log-only-Backup machen.

- **-behalten-archivelog-Backups -Stunden- -Tage- Wochen- Monthsmonths**

  Gibt an, dass die Archiv-Log-Backups auf Basis der Aufbewahrungsdauer des Archivprotokolls aufbewahrt werden (stündlich, täglich, wöchentlich, monatlich).

- **Schutz [-Schutz-policypolicy_Name] -noprotect**

  Gibt an, dass die Archivprotokolldateien auf der Grundlage der Archivierungsprotokollschutzrichtlinie geschützt werden.

  Die Option -noprotect gibt an, dass die Archivprotokolldateien nicht geschützt werden sollen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

- **-include-with-online-Backups**

  Gibt an, dass das Backup des Archivprotokolls zusammen mit dem Online-Datenbank-Backup enthalten ist.

- **-no-include-with-online-Backups**

  Gibt an, dass die Archiv-Log-Backups nicht zusammen mit dem Online-Datenbank-Backup enthalten sind.

- **-dump**

  Gibt an, dass die Dump-Dateien nach dem erfolgreichen Erstellen des Profils gesammelt werden.

Beispiel

Das folgende Beispiel zeigt die Erstellung eines Profils mit stündlicher Aufbewahrungsrichtlinie und E-Mail-Benachrichtigung:

```
smo profile create -profile test_rbac -profile-password netapp -repository
-dbname SMOREP -host hostname.org.com -port 1521 -login -username smorep
-database -dbname
RACB -host saal -sid racb1 -login -username sys -password netapp -port
1521 -rman -controlfile -retain -hourly -count 30 -verbose
Operation Id [8abc01ec0e78ebda010e78ebe6a40005] succeeded.
```

Verwandte Informationen

Profilverwaltung für effiziente Backups

Der Befehl smo Protection-Policy

Benennen von Snapshot-Kopien

Wie SnapManager Backups auf dem lokalen Storage aufbewahrt

Der Befehl smoprofile delete

Sie können den Befehl „Profil löschen“ ausführen, um ein Profil der Datenbank zu löschen.

Syntax

```
        smo profile delete
-profile profile
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt das zu löschende Profil an.

- **-ruhig**

Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Profil gelöscht:

```
smo profile delete -profile SALES1
Operation Id [Ncaf00af0242b3e8dba5c68a57a5ae932] succeeded.
```

Verwandte Informationen

Profile werden gelöscht

Der Befehl smo profile destroy

Dieser Befehl löscht den Split Clone (Datenbank) zusammen mit dem Profil, das von SnapManager während des Klon-Split-Prozesses generiert wurde.

Syntax

```
        smo profile destroy
-profile profile
\[-host hostname\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt das Profil an, das SnapManager nach einem erfolgreichen Klonteilungsprozess generiert.

- **-Host-Hostname**

  Gibt den Hostnamen an, in dem der geteilte Klon vorhanden ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel wird das Profil SALES1 gelöscht.

```
smo profile destroy -profile SALES1
```

Der Befehl smoprofile dump

Sie können den Profildump-Befehl ausführen, um die .jar-Datei zu erstellen, die Diagnoseinformationen zu einem Profil enthält.

Syntax

```
        smo profile dump
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie die Speicherauszugsdateien erstellen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird ein Dump für das Profil SALES1 erstellt:

```
smo profile dump -profile SALES1
Dump file created
Path:/userhomedirectory/.netapp/smo/3.3.0/smo_dump_SALES1_hostname.jar
```

Der Befehl smo profile list

Mit diesem Befehl wird eine Liste der aktuellen Profile angezeigt.

Syntax

```
        smo profile list
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden vorhandene Profile mit ihren Details angezeigt.

```
smo profile list -verbose
Profile name: FGTER
Repository:
  Database name: SMOREPO
  SID: SMOREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: ********
Profile name: TEST_RBAC
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: TEST_RBAC_DP_PROTECT
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: TEST_HOSTCREDEN_OFF
Repository:
```

```
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: SMK_PRF
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: FGLEX
Repository:
  Database name: SMOREPO
  SID: SMOREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: ********
```

Der Befehl smo profile show

Sie können den Befehl „Profile show“ ausführen, um die Informationen zu einem Profil anzuzeigen.

Syntax

```
        smo profile show
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel werden die Details des Profils angezeigt:

```
smo profile show -profile TEST_RBAC_DP_PROTECT -verbose
Profile name: TEST_RBAC_DP_PROTECT
Comment:
Target database:
  Database name: racb
  SID: racb1
  Host: saal
  Port: 1521
  Username: sys
  Password: ********
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
RMAN:
  Use RMAN via control file
Oracle user account: oracle
Oracle user group: dba
Snapshot Naming:
  Pattern: smo_{profile}_{db-sid}_{scope}_{mode}_{smid}
  Example:
smo_test_rbac_dp_protect_racb1_f_h_1_8abc01e915a55ac50115a55acc8d0001_0
Protection:
  Dataset: smo_saal_racb
  Protection policy: Back up
  Conformance status: CONFORMANT
Local backups to retain:
  Hourly: 4 copies
  Daily: 7 day(s)
  Weekly: 4 week(s)
  Monthly: 12 month(s)
```

Der Befehl smo profile SYNC

Mit diesem Befehl werden die Profile-to-Repository-Zuordnungen für dieses Repository in eine Datei im Home-Verzeichnis auf dem lokalen Host geladen.

Syntax

```
        smo profile sync
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login
-username repo_username
                \[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt die Repository-Datenbank für das zu synchronisierende Profil an.

- **-Host**

  Gibt den Datenbank-Host an.

- **-Port**

  Gibt den Port für den Host an.

- **-Login**

  Gibt den Anmeldeprozess für den Hostbenutzer an.

- **-username**

  Gibt den Benutzernamen für den Host an.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel zeigt das Ergebnis des Befehls zum Synchronisieren der Profile-zu-Repository-Zuordnungen für die Datenbank.

```
smo profile sync -repository -dbname smrepo -host Host2 -port 1521 -login
-username user2
SMO-12345 [INFO ]: Loading profile mappings for repository
"user2@Host2:smrepo" into cache for OS User "admin".
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

Der Befehl smoprofile Update

Sie können den Befehl „Profilaktualisierung“ ausführen, um die Informationen für ein vorhandenes Profil zu aktualisieren.

Syntax

```
        smo profile update
-profile profile
\[-new-profile new_profile_name\]
\[-profile-password profile_password\]
[-database
-dbname db_dbname
-host db_host
\[-sid db_sid\]
[-login
\[-username db_username -password db_password -port db_port\]
 \[-asminstance -asmusername asminstance_username  -asmpassword
asminstance_password\]]
[\{-rman  \{-controlfile \| \{\{-login
-username  rman_username
-password  rman_password \}
\[-tnsname  tnsname\]\}\}\} \|
-remove-rman\]
-osaccount osaccount
-osgroup osgroup
[-retain
\[-hourly \[-count n\] \[-duration m\]\]
\[-daily \[-count n\] \[-duration m\]]
\[-weekly \[-count n\] \[-duration m\]]
\[-monthly \[-count n\] \[-duration m\]]]]
-comment comment
-snapname-patternpattern
[-protect \[-protection-policy policy_name\] \| \[-noprotect\]]
[-summary-notification]
[-notification
\[-success
-email email_address1,email_address2
-subject subject_pattern\]
\[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups
-retain-archivelog-backups
-hours  hours |
-days days |
-weeks weeks |
-months months
[-protect \[-protection-policy policy_name\] \| \[-noprotect\]]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
\[-quiet \| -verbose\]
```

Parameter

Wenn eine Schutzrichtlinie für das Profil festgelegt wurde, kann die Richtlinie nicht mit SnapManager geändert werden. Sie müssen die Richtlinie mithilfe der Protection Manager-Konsole ändern.

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-profile-password Profil_password**

  Gibt das Kennwort für das Profil an.

- **-New-profile New_profile_Name**

  Gibt den neuen Namen an, den Sie für ein Profil angeben können.

- **-Datenbank**

  Gibt die Details der Datenbank an, die das Profil beschreibt. Diese Datenbank wird gesichert, wiederhergestellt usw.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Datenbank ausgeführt wird.

- **-sid db_sid**

  Gibt die Systemkennung der Datenbank an, die das Profil beschreibt. Standardmäßig verwendet SnapManager den Datenbanknamen als Systemkennung. Falls sich die Systemkennung vom Datenbanknamen unterscheidet, müssen Sie sie mit der Option -sid angeben.

  Wenn Sie beispielsweise Oracle Real Application Clusters (RAC) verwenden, müssen Sie die SID-Systemkennung der RAC-Instanz auf dem RAC-Knoten angeben, von dem aus SnapManager ausgeführt wird.

- **-Login**

  Gibt die Anmeldedaten für das Repository an.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Datenbank**

Gibt die Details der Datenbank an, die das Profil beschreibt. Diese Datenbank wird gesichert, wiederhergestellt und geklont.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Datenbank ausgeführt wird.

- **-Login**

  Gibt die Anmeldedaten für die Datenbank an.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Port db_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-asminstance**

  Gibt die Anmeldeinformationen an, die zur Anmeldung bei der Instanz für die automatische Speicherverwaltung (ASM) verwendet werden.

- **-asmusername asminstance_username**

  Gibt den Benutzernamen an, der zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-asmpassword asminstance_password**

  Gibt das Kennwort an, das zur Anmeldung bei der ASM-Instanz verwendet wird.

- **-rman**

  Gibt die Details an, die SnapManager zum Katalogisieren von Backups mit dem Oracle Recovery Manager (RMAN) verwendet.

- **-controlfile**

  Gibt die Steuerdateien für die Zieldatenbank an, anstatt einen Katalog als RMAN-Repository zu verwenden.

- **-Login**

  Gibt die RMAN-Anmeldedaten an.

- **-Passwort rman_password**

  Gibt das Kennwort an, mit dem Sie sich beim RMAN-Katalog anmelden können.

- **-username rman_Benutzername**

  Gibt den Benutzernamen an, der zum Anmelden beim RMAN-Katalog verwendet wird.

- **-tnsname tnsname**

  Gibt den Verbindungsnamen tnsname an (dieser wird in der Datei tsname.ora definiert).

- **-remove-rman**

  Legt fest, dass RMAN im Profil entfernt wird.

- **-osaccount osconcount**

  Gibt den Namen des Benutzerkontos für die Oracle-Datenbank an. SnapManager verwendet dieses Konto, um die Oracle-Vorgänge wie dem Starten und Herunterfahren durchzuführen. Normalerweise ist es der Benutzer, der die Oracle-Software auf dem Host besitzt, zum Beispiel oracle.

- **-osgroup osgroup**

  Gibt den Namen der Oracle-Datenbankgruppe an, die dem oracle-Konto zugeordnet ist.

- **-behalten [-hourly [-countn] [-duration m] [-taily [-count n] [-duration m]] [-Weekly [-count n][-duration m]] [-monthly [-count n][-duration m]]**

  Gibt die Aufbewahrungsklasse (stündlich, täglich, wöchentlich, monatlich) für ein Backup an.

  Für jede Aufbewahrungsklasse kann ein Aufbewahrungszähler oder eine Aufbewahrungsdauer oder beides angegeben werden. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunden oder Tage für täglich). Wenn der Benutzer beispielsweise nur eine Aufbewahrungsdauer von 7 für tägliche Backups angibt, dann wird SnapManager nicht die Anzahl der täglichen Backups für das Profil begrenzen (da die Aufbewahrungsanzahl 0 ist), aber SnapManager löscht automatisch täglich erstellte Backups, die vor 7 Tagen erstellt wurden.

- **-Kommentar**

  Gibt den Kommentar für ein Profil an.

- **-snapname-Muster**

  Gibt das Benennungsmuster für Snapshot Kopien an. Außerdem können Sie in allen Namen von Snapshot Kopien benutzerdefinierten Text einfügen, beispielsweise HAOPS für hochverfügbare Vorgänge. Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht aufgetreten sind. Snapshot Kopien, die vorhanden sind, behalten das vorherige SnapName-Muster bei. Sie können mehrere Variablen im Mustertext verwenden.

- **-Protect [-Protection-policypolicy_Name]**

  Gibt an, ob das Backup auf einem sekundären Storage gesichert werden soll oder nicht.

Wenn -protect ohne -Protection-Policy angegeben wird, dann hat der Datensatz keine Schutzpolitik. Wenn -protect angegeben wird und -Protection-Policy beim Erstellen des Profils nicht gesetzt wird, dann kann es später mit dem Befehl bysmo profile Update gesetzt oder vom Speicheradministrator über die Konsole des Protection Manager eingestellt werden.

Die Option -noprotect gibt an, dass das Profil nicht auf den sekundären Speicher geschützt wird.

- **-summary-notification**

  Gibt an, dass die E-Mail-Benachrichtigung für das vorhandene Profil aktiviert ist.

- **-Mitteilung [-success-email e-Mail_adress1,E-Mail address2 -subject_pattern]**

  Aktiviert die E-Mail-Benachrichtigung für das vorhandene Profil, sodass die Empfänger nach erfolgreicher SnapManager-Operation E-Mails erhalten. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den Betreff der E-Mail für das vorhandene Profil.

  Sie können den Betreff während der Aktualisierung des Profils ändern oder benutzerdefinierten Text einfügen. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-Benachrichtigung [-Failure -Email-adress1,E-Mail address2 -subject_pattern]**

  Aktiviert die E-Mail-Benachrichtigung für das vorhandene Profil, sodass die Empfänger bei Ausfall des SnapManager-Vorgangs E-Mails erhalten. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den Betreff der E-Mail für das vorhandene Profil.

  Sie können den Betreff während der Aktualisierung des Profils ändern oder benutzerdefinierten Text einfügen. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-separate-archivlog-Backups**

  Trennt das Backup des Archivprotokolls von der Datendatei-Sicherung. Dies ist ein optionaler Parameter, den Sie beim Erstellen des Profils angeben können. Nachdem Sie die Backups mit dieser Option getrennt haben, können Sie entweder Datendateien-only-Backup oder Archiv-Log-only-Backup erstellen.

- **-behalten-archivelog-Backups -Stunden- -Tage- Wochen- Monthsmonths**

  Gibt an, dass die Archiv-Log-Backups auf Basis der Aufbewahrungsdauer des Archivprotokolls aufbewahrt werden (stündlich, täglich, wöchentlich, monatlich).

- **-Protect [-Protection-policypolicy_Name] -noprotect**

  Gibt an, dass die Archivprotokolldateien auf der Grundlage der Archivierungsprotokollschutzrichtlinie geschützt sind.

  Gibt an, dass die Archivprotokolldateien nicht mit der Option -noprotect geschützt sind.

- **-enthalten-mit-online-Backups**

  Gibt an, dass das Backup des Archivprotokolls zusammen mit dem Online-Datenbank-Backup enthalten

ist.

Gibt an, dass die Archiv-Log-Backups nicht zusammen mit dem Online-Datenbank-Backup enthalten sind.

- **-dump**

  Gibt an, dass die Dump-Dateien nach dem erfolgreichen Erstellen des Profils gesammelt werden.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel werden die Anmeldeinformationen für die im Profil beschriebene Datenbank geändert und die E-Mail-Benachrichtigung ist für dieses Profil konfiguriert:

```
smo profile update -profile SALES1 -database -dbname SALESDB
 -sid SALESDB -login -username admin2 -password d4jPe7bw -port 1521
-host server1 -profile-notification -success -e-mail Preston.Davis@org.com
-subject success
Operation Id [8abc01ec0e78ec33010e78ec3b410001] succeeded.
```

Verwandte Informationen

Profilkennwörter werden geändert

Wie SnapManager Backups auf dem lokalen Storage aufbewahrt

Der Befehl smoprofile verify

Sie können den Befehl „Profile Verify“ ausführen, um die Einrichtung des Profils zu überprüfen. Sie müssen die Datenbank mounten, bevor Sie diesen Befehl ausführen.

Syntax

```
        smo profile verify
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

Gibt das zu überprüfenden Profil an. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Profil überprüft:

```
smo profile verify -profile test_profile  -verbose
[ INFO] SMO-07431: Saving starting state of the database: racb1(OPEN).
[ INFO] SMO-07431: Saving starting state of the database: racb2(SHUTDOWN),
racb1(OPEN).
[ INFO] SD-00019: Discovering storage resources for all system devices.
[ INFO] SD-00020: Finished storage discovery for all system devices.
[ INFO] SD-00019: Discovering storage resources for all system devices.
[ INFO] SD-00020: Finished storage discovery for all system devices.
[ INFO] SD-00019: Discovering storage resources for all system devices.
[ INFO] SD-00020: Finished storage discovery for all system devices.
[ INFO] SMO-05070: Database profile test_profile is eligible for fast
restore.
[ INFO] SMO-07433: Returning the database to its initial state:
racb2(SHUTDOWN), racb1(OPEN).
[ INFO] SMO-13048: Profile Verify Operation Status: SUCCESS
[ INFO] SMO-13049: Elapsed Time: 0:04:14.919
Operation Id [Nfffde14ac88cd1a21597c37e8d21fe90] succeeded.
```

Verwandte Informationen

Profile werden überprüft

Der Befehl smo Protection-Policy

Mit dem Befehl „Protection-Policy“ können Sie die Sicherheitsrichtlinien auflisten, die auf ein Profil angewendet werden können. Die Schutzrichtlinie kann angewendet werden, wenn ein neues Profil erstellt oder ein vorhandenes Profil aktualisiert wird. Sie können auch die Sicherungsrichtlinie für das Profil über die Protection Manager Konsole festlegen.

Syntax

```
smo protection-policy list
```

Protection Manager und SnapDrive müssen auf dem Server installiert sein, damit Sie diesen Befehl verwenden können.

Parameter

- **Liste**

  Zeigt die Liste der Schutzrichtlinien an, die in einem Profil festgelegt werden können.

Beispiel

Im folgenden Beispiel werden die Sicherungsrichtlinien aufgeführt, die auf ein Profil festgelegt werden können:

```
smo protection-policy list
```

```
Back up
Back up, then mirror
Chain of two mirrors
DR Back up
DR Back up, then mirror
DR Mirror
DR Mirror and back up
DR Mirror and mirror
DR Mirror, then back up
DR Mirror, then mirror
Local backups only
Mirror
Mirror and back up
Mirror to two destinations
Mirror, then back up
No protection
Partial-volume Mirror
Remote backups only
```

Verwandte Informationen

Profilverwaltung für effiziente Backups

Der Befehl smo Repository create

Syntax

Mit diesem Befehl wird ein Repository erstellt, in dem Datenbankprofile und zugehörige Anmeldedaten gespeichert werden. Dieser Befehl überprüft außerdem, ob die Blockgröße geeignet ist.

```
        smo repository create
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Erstellung des Repositorys zu erzwingen. Wenn Sie diese Option verwenden, werden Sie von SnapManager aufgefordert, das Repository zu sichern, bevor Sie das Repository erstellen.

- **-noprompt**

  Zeigt nicht die Aufforderung zum Sichern des Repository vor der Erstellung an, wenn Sie die Option -Force verwenden. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt

wird. Dies erleichtert das Erstellen von Repositories mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Befehlsbeispiel

Im folgenden Beispiel wird ein Repository in der Datenbank SMOREPO auf dem Host hotspur erstellt.

```
smo repository create -repository -port 1521 -dbname SMOREPO -host hotspur
-login -username grabal21 -verbose
SMO-09202 [INFO ]: Creating new schema as grabal21 on
jdbc:oracle:thin:@//hotspur:1521/SMOREPO.
SMO-09205 [INFO ]: Schema generation complete.
SMO-09209 [INFO ]: Performing repository version INSERT.
SMO-09210 [INFO ]: Repository created with version: 30
SMO-13037 [INFO ]: Successfully completed operation: Repository Create
SMO-13049 [INFO ]: Elapsed Time: 0:00:08.844
```

Der Befehl smo Repository löschen

Mit diesem Befehl wird ein Repository gelöscht, das zum Speichern von Datenbankprofilen und zugehörigen Anmeldedaten verwendet wird. Sie können ein Repository nur löschen, wenn kein Profil im Repository vorhanden ist.

Syntax

```
        smo repository delete
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Force**

  Versucht, das Löschen des Repositorys zu erzwingen, auch wenn unvollständige Vorgänge vorliegen. SnapManager gibt eine Eingabeaufforderung aus, wenn unvollständige Vorgänge vorliegen. Sie werden gefragt, ob Sie das Repository wirklich löschen möchten.

- **-noprompt**

  Fordert Sie nicht auf, bevor Sie das Repository löschen. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert das Löschen von Repositorys mit einem Skript.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Befehlsbeispiel

Im folgenden Beispiel wird das Repository in der SALESDB-Datenbank gelöscht.

```
smo repository delete -repository -port 1521 -dbname smorep
-host nila -login -username smofresno -force -verbose
This command will delete repository "smofresno@smorep/nila".
Any resources maintained by the repository must be cleaned up manually.
This may include snapshots, mounted backups, and clones.
Are you sure you wish to proceed (Y/N)?Y
[ INFO] SMO-09201: Dropping existing schema as smofresno
  on jdbc:oracle:thin:@//nila:1521/smorep.
[ INFO] SMO-13048: Repository Delete Operation Status: SUCCESS
[ INFO] SMO-13049: Elapsed Time: 0:00:06.372
[ INFO] SMO-20010: Synchronizing mapping for profiles in
   repository "smofresno@smorep/nila:1521".
[ WARN] SMO-20029: No repository schema exists in
"smofresno@smorep/nila:1521".
 Deleting all profile mappings for this repository.
[ INFO] SMO-20012: Deleted stale mapping for profile "TESTPASS".
```

Der smo Repository Rollback-Befehl

Mit diesem Befehl können Sie ein Rollback oder ein Zurücksetzen einer höheren Version von SnapManager auf die Originalversion, von der Sie das Upgrade durchgeführt haben, durchführen.

Syntax

```
        smo repository rollback
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-rollbackhost host_with_target_database
[-force]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-rollbackhost Host_with_target_Database**

  Gibt den Namen des Hosts an, der von einer höheren Version von SnapManager auf die ursprüngliche niedrigere Version zurückgesetzt wird.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Aktualisierung des Repositorys zu erzwingen. SnapManager fordert Sie auf, vor der Aktualisierung eine Sicherung des aktuellen Repository durchzuführen.

- **-noprompt**

  Zeigt die Eingabeaufforderung nicht an, bevor die Repository-Datenbank aktualisiert wird. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert die Aktualisierung von Repositorys mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel aktualisiert das Repository in der SALESDB-Datenbank.

```
smo repository rollback -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -rollbackhost hostA
```

Der Befehl smo Repository Rolling Upgrade

Mit diesem Befehl wird das Upgrade auf einen einzelnen oder mehrere Hosts und die zugehörigen Zieldatenbanken durchgeführt – von einer niedrigeren Version von SnapManager auf eine höhere Version. Der aktualisierte Host wird nur mit der höheren Version von SnapManager verwaltet.

Syntax

```
        smo repository rollingupgrade
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-upgradehost host_with_target_database
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Upgradehost Host_with_Target_Database**

  Gibt den Namen des Hosts an, der von einer niedrigeren Version von SnapManager auf eine höhere Version aktualisiert wird.

- **-Port repo_Port**

Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Aktualisierung des Repositorys zu erzwingen. SnapManager fordert Sie auf, vor der Aktualisierung eine Sicherung des aktuellen Repository durchzuführen.

- **-noprompt**

  Zeigt die Eingabeaufforderung nicht an, bevor die Repository-Datenbank aktualisiert wird. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert die Aktualisierung von Repositorys mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel aktualisiert das Repository in der SALESDB-Datenbank.

```
smo repository rollingupgrade -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -upgradehost hostA
```

Der Befehl smo Repository show

Mit diesem Befehl werden Informationen zum Repository angezeigt.

Syntax

```
        smo repository show
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Befehlsbeispiel

Das folgende Beispiel zeigt Details zum Repository in der SALESDB-Datenbank.

```
smo repository show -repository -dbname SALESDB -host server1
-port 1521 -login -username admin
Repository Definition:
User Name: admin
Host Name: server1
Database Name: SALESDB
Database Port: 1521
Version: 28
Hosts that have run operations using this repository: 2
server2
server3
Profiles defined in this repository: 2
GSF5A
GSF3A
Incomplete Operations: 0
```

Der Befehl smo Repository Update

Mit diesem Befehl wird das Repository aktualisiert, in dem Datenbankprofile und die zugehörigen Anmeldedaten gespeichert werden, wenn Sie ein SnapManager-Upgrade durchführen. Wenn Sie eine neue Version von SnapManager installieren, müssen Sie den Befehl Repository Update ausführen, bevor Sie die neue Version verwenden können. Sie können diesen Befehl nur verwenden, wenn im Repository keine unvollständigen Befehle vorhanden sind.

Syntax

```
        smo repository update
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den

globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Aktualisierung des Repositorys zu erzwingen. SnapManager fordert Sie auf, vor der Aktualisierung eine Sicherung des aktuellen Repository durchzuführen.

- **-noprompt**

  Zeigt die Eingabeaufforderung nicht an, bevor die Repository-Datenbank aktualisiert wird. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert die Aktualisierung von Repositorys mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel aktualisiert das Repository in der SALESDB-Datenbank.

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521
```

Der Befehl smo schedule create

Sie können mit dem Befehl „Schedule create“ ein Backup zu einem bestimmten Zeitpunkt planen.

Syntax

```
        smo schedule create
-profile profile_name
\[-full\{-auto \| -online \| -offline\}
\[-retain -hourly \| -daily \| -weekly \| -monthly \| -unlimited\]
\[-verify\]\] |
\[-data \[\[-files files \[files\]\] \|
\[-tablespaces tablespaces \[tablespaces\]\] \{-auto \| -online \|
-offline\}
\[-retain -hourly \| -daily \| -weekly \| -monthly \| -unlimited\]
\[-verify\]\] |
\[-archivelogs\]}
\[-label label\]
\[-comment comment\]
\[-protect \| -noprotect \| -protectnow\]
\[-backup-dest path1 \[ , path2\]\]
\[-exclude-dest path1 \[ , path2\]\]
\[-prunelogs \{-all \| -until-scn until-scn \| -until -date  yyyy-MM-
dd:HH:mm:ss\] \| -before \{-months \| -days \| -weeks \| -hours}}
-prune-dest prune_dest1,\[prune_dest2\]\]
-schedule-name schedule_name
\[-schedule-comment schedule_comment\]
-interval \{-hourly \| -daily \| -weekly \| -monthly \| -onetimeonly\}
-cronstring cron_string
-start-time \{start_time <yyyy-MM-dd HH:mm\>\}
-runasuser runasuser
\[-taskspec taskspec\]
-force
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, für die das Backup geplant werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Auto Option**

  Wenn die Datenbank im Status „angehängt“ oder „Offline“ steht, führt SnapManager ein Offline-Backup durch. Wenn sich die Datenbank im offenen oder Online-Status befindet, führt SnapManager ein Online-Backup durch. Wenn Sie die Option -Force mit der Option -offline verwenden, erzwingt SnapManager ein Offline-Backup, selbst wenn die Datenbank derzeit online ist.

- **-Online-Option**

  Gibt ein Online-Datenbank-Backup an.

Sie können ein Online-Backup einer RAC-Datenbank (Real Application Clusters) erstellen, solange sich der primäre Status im offenen oder gemounteten Zustand befindet und sich eine Instanz im offenen Zustand befindet. Sie können die Option -Force für Online-Backups verwenden, wenn sich die lokale Instanz im Shutdown-Status befindet oder keine Instanz geöffnet ist.

  - Wenn sich die lokale Instanz im Status beim Herunterfahren befindet und mindestens eine Instanz geöffnet ist, können Sie die Option -Force verwenden, um die lokale Instanz in angehängt zu ändern.
  - Wenn sich keine Instanz im offenen Status befindet, können Sie die Option -Force verwenden, um die lokale Instanz zum Öffnen zu ändern.

- **-Offline-Option**

  Gibt eine Offline-Sicherung an, während sich die Datenbank im Shutdown-Status befindet. Wenn sich die Datenbank im offenen oder gemounteten Status befindet, schlägt das Backup fehl. Wenn die Option -Force verwendet wird, versucht SnapManager, den Datenbankstatus zu ändern, um die Datenbank für ein Offline-Backup herunterzufahren.

- **-Volloption**

  Sicherung der gesamten Datenbank. Dazu gehören alle Daten, archivierte Log- und Kontrolldateien. Die archivierten Wiederherstellungsprotokolle und Kontrolldateien werden gesichert, unabhängig davon, welche Art von Backup Sie durchführen. Wenn Sie nur einen Teil der Datenbank sichern möchten, verwenden Sie die Option -files oder -Tablespaces.

- **-Dateiliste**

  Sichert nur die angegebenen Datendateien sowie die archivierten Protokoll- und Kontrolldateien. Trennen Sie die Liste der Dateinamen mit Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * -Tablespaces*

  Sicherung nur der angegebenen Datenbanktablespaces plus der archivierten Protokoll- und Kontrolldateien Trennen Sie die Namen der Tablespaces durch Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * Name des Etiketts*

  Gibt einen optionalen Namen für dieses Backup an. Dieser Name muss innerhalb des Profils eindeutig sein. Der Name kann Buchstaben, Zahlen, Unterstrich (_) und Bindestrich (-) enthalten. Es kann nicht mit einem Bindestrich beginnen.

  Wenn Sie keine Beschriftung angeben, erstellt SnapManager im Scope_type_date-Format eine Standardbeschriftung:

  - Der Umfang ist entweder F, um ein vollständiges Backup anzuzeigen, oder P, um auf ein teilweises Backup hinzuweisen.
  - Geben Sie C ein, um ein Offline-Backup (Cold) anzuzeigen, H für ein Online-Backup (Hot) oder Ein Für die automatische Sicherung, z. B. P_A_20081010060037IST, anzuzeigen.
  - Datum ist Jahr, Monat, Tag und Uhrzeit des Backups.

    SnapManager verwendet eine 24-Stunden-Zeit.

  Beispiel: Wenn Sie am 16. Januar 2007 um 5:45:16 Uhr eine vollständige Sicherung mit offline der

Datenbank durchgeführt haben Eastern Standard Time, SnapManager würde die Bezeichnung F_C_20070116174516EST erstellen.

- **-comment-Zeichenfolge**

  Gibt einen optionalen Kommentar an, um dieses Backup zu beschreiben. Schließen Sie den String in einzelne Anführungszeichen (').

  > Einige Schalen Streifen Anführungszeichen ab. Wenn dies für Ihre Shell zutrifft, müssen Sie das Anführungszeichen mit einem umgekehrten Schrägstrich (\) angeben. Beispielsweise müssen Sie Folgendes eingeben: `\' this is a comment\'`.

- **-Verify Option**

  Überprüft, ob die Dateien im Backup nicht beschädigt sind, indem Sie das Oracle dbv-Dienstprogramm ausführen.

  > Wenn Sie die Option -verify angeben, wird der Backup-Vorgang erst abgeschlossen, wenn der Überprüfungvorgang abgeschlossen ist.

- **-Force Option**

  Erzwingt eine Statusänderung, wenn sich die Datenbank nicht im richtigen Zustand befindet. Beispielsweise kann SnapManager den Status der Datenbank von Online- in Offline-Modus ändern, basierend auf dem von Ihnen angegebenen Backup-Typ und dem Status, in dem sich die Datenbank befindet.

  Verwenden Sie bei einem Online-Backup der RAC-Datenbank die Option -Force, wenn die lokale Instanz heruntergefahren ist oder keine Instanz geöffnet ist.

  > Die Version von Oracle muss 10.2.0.5 sein. Andernfalls wird die Datenbank hängen, wenn eine Instanz im RAC eingebunden ist.

  - Wenn die lokale Instanz sich im Shutdown-Status befindet und mindestens eine Instanz geöffnet ist, können Sie die lokale Instanz mithilfe der Option -Force auf gemountet ändern.
  - Wenn keine Instanz geöffnet ist, können Sie die lokale Instanz durch Verwenden der Option -Force auf Öffnen ändern.

- * -Schutz *

  Gibt an, ob das Backup auf sekundärem Storage gesichert werden soll. Die Option -noprotect gibt an, dass das Backup nicht auf einem sekundären Speicher geschützt werden soll. Nur vollständige Backups sind gesichert. Wenn keine Option angegeben wird, schützt SnapManager das Backup standardmäßig, wenn es sich bei dem Backup um ein vollständiges Backup handelt, und das Profil eine Schutzrichtlinie angibt. Die Option -protectnow gilt nur für Data ONTAP im 7-Mode. Die Option gibt an, dass das Backup sofort auf dem sekundären Storage geschützt ist.

- **-halten Sie { - stündlich - jeden Tag — monatlich - unbegrenzt}**

  Gibt an, ob das Backup stündlich, täglich, wöchentlich, monatlich oder unbegrenzt aufbewahrt werden soll. Wenn die Option -Retention nicht angegeben ist, wird die Aufbewahrungsklasse standardmäßig auf -hourly gesetzt. Mit der Option -unlimited können Sie Backups für immer aufbewahren. Die Option -unlimited macht das Backup nicht zur Löschung durch die Aufbewahrungsrichtlinie.

- **-Archivprotokolle**

  Gibt die Erstellung eines Backup-Protokolls für das Archivprotokoll an.

- **-Backup-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll für die Sicherung des Archivprotokolls an.

- **-exclude-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll an, die vom Backup ausgeschlossen werden sollen.

- *-prunelogs {-all} -bis-scnbis-scn - bis-dateyyyyy-MM-dd:HH:mm:ss - vor {-Monaten

  Gibt an, ob die Archivprotokolldateien aus den Speicherprotokollzielen gelöscht werden sollen, basierend auf den beim Erstellen eines Backups bereitgestellten Optionen. Die Option -all löscht alle Archivprotokolldateien aus den Archivprotokollzielen. Mit der Option -bis-scn werden die Archivprotokolldateien bis zu einer angegebenen Systemändernummer (SCN) gelöscht. Mit der Option -bis -date werden die Archivprotokolldateien bis zum angegebenen Zeitraum gelöscht. Die Option -before löscht die Archivprotokolldateien vor dem angegebenen Zeitraum (Tage, Monate, Wochen, Stunden).

- **-Schedule-Name schedule_Name**

  Gibt den Namen an, den Sie für den Zeitplan angeben.

- **-schedule-comment schedule_comment**

  Gibt einen optionalen Kommentar an, um die Planung des Backups zu beschreiben.

- **-Intervall { -stündlich} -täglich / -wöchentlich / -ontimeonly**

  Gibt das Zeitintervall an, mit dem die Backups erstellt werden. Sie können das Backup stündlich, täglich, wöchentlich, monatlich oder einmalig planen.

- **-cronstring cron_string**

  Gibt die Planung des Backups mithilfe von cronstring an. Cron-Ausdrücke werden verwendet, um Instanzen von CronTrigger zu konfigurieren. Cron-Ausdrücke sind Zeichenfolgen, die aus den folgenden Unterausdrücken bestehen:

  - 1 bezieht sich auf Sekunden.
  - 2 bezieht sich auf Minuten.
  - 3 bezieht sich auf Stunden.
  - 4 bezieht sich auf einen Tag im Monat.
  - 5 bezieht sich auf den Monat.
  - 6 bezieht sich auf einen Tag in einer Woche.
  - 7 bezieht sich auf das Jahr (optional).

- **-Startzeit yyyy-MM-dd HH:mm**

  Gibt die Startzeit des geplanten Vorgangs an. Die Startzeit des Zeitplans sollte im Format yyyy-MM-dd HH:mm enthalten sein.

- **-runasuser runasuser**

  Gibt an, dass der Benutzer (Root-Benutzer oder Oracle-Benutzer) des geplanten Backup-Vorgangs während der Planung des Backups geändert wird.

- **-taskSpec taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation an, die für die Vorverarbeitung oder Nachverarbeitung des Backup-Vorgangs verwendet werden kann. Der vollständige Pfad der XML-Datei muss mit der Option -taskSpec bereitgestellt werden.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Der Befehl smo schedule delete

Durch diesen Befehl wird ein Backup-Zeitplan gelöscht, wenn er nicht mehr benötigt wird.

Syntax

```
        smo schedule delete
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die Sie einen Backup-Zeitplan löschen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Planungsnamen an, den Sie beim Erstellen eines Backup-Zeitplans angegeben haben.

Der Befehl smo schedule list

Mit diesem Befehl werden die geplanten Vorgänge aufgelistet, die einem Profil zugeordnet sind.

Syntax

```
        smo schedule list
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils für die Datenbank an, mit dem Sie eine Liste geplanter Vorgänge anzeigen können. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

Der Smo Schedule Resume Befehl

Mit diesem Befehl wird der ausgesetzt gesperrte Backup-Zeitplan fortgesetzt.

Syntax

```
        smo schedule resume
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die den unterbrochenen Backup-Zeitplan fortsetzen soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Planungsnamen an, den Sie beim Erstellen eines Backup-Zeitplans angegeben haben.

Der Befehl smoplan suspendieren

Mit diesem Befehl wird ein Backup-Zeitplan so lange unterbrochen, bis der Backup-Zeitplan wieder aufgenommen wird.

Syntax

```
        smo schedule suspend
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die einen Backup-Zeitplan aussetzen soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Planungsnamen an, den Sie beim Erstellen eines Backup-Zeitplans angegeben haben.

Der Befehl smo schedule Update

Mit diesem Befehl wird der Zeitplan für ein Backup aktualisiert.

Syntax

```
        smo schedule update
-profile profile_name
-schedule-name schedule_name
\[-schedule-comment schedule_comment\]
-interval \{-hourly \| -daily \| -weekly \| -monthly \| -onetimeonly\}
-cronstring cron_string
-start-time \{start_time <yyyy-MM-dd HH:mm\>\}
-runasuser runasuser
\[-taskspec taskspec\]
-force
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die die Sicherung planen soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Namen an, den Sie für den Zeitplan angeben.

- **-schedule-comment schedule_comment**

  Gibt einen optionalen Kommentar an, um die Planung des Backups zu beschreiben.

- **-Intervall { -stündlich} -täglich / -wöchentlich / -ontimeonly**

  Gibt das Zeitintervall an, mit dem die Backups erstellt werden. Sie können das Backup nur stündlich, täglich, wöchentlich, monatlich oder einmalig planen.

- **-cronstring cron_string**

Gibt an, das Backup mit cronstring zu planen. Cron-Ausdrücke werden verwendet, um Instanzen von CronTrigger zu konfigurieren. Cron-Ausdrücke sind Zeichenfolgen, die tatsächlich aus sieben Unterausdrücken bestehen:

- 1 bezieht sich auf Sekunden
- 2 bezieht sich auf Minuten
- 3 bezieht sich auf Stunden
- 4 bezieht sich auf einen Tag im Monat
- 5 bezieht sich auf den Monat
- 6 bezieht sich auf einen Tag in einer Woche
- 7 bezieht sich auf das Jahr (optional)

- **-Startzeit yyyy-MM-dd HH:mm**

  Gibt die Startzeit des Zeitplanvorgangs an. Die Startzeit des Zeitplans sollte im Format yyyy-MM-dd HH:mm enthalten sein.

- **-runasuser runasuser**

  Gibt an, den Benutzer des geplanten Backup-Vorgangs während der Planung des Backups zu ändern.

- **-taskSpec taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation an, die für die Vorverarbeitung oder Nachverarbeitung des Backup-Vorgangs verwendet werden kann. Der vollständige Pfad der XML-Datei sollte zur Verfügung gestellt werden, die die Option -taskSpec geben.

Der Befehl smo Storage list

Sie können den Befehl Storage list ausführen, um die Liste der Speichersysteme anzuzeigen, die einem bestimmten Profil zugeordnet sind.

Syntax

```
        smo storage list
-profile profile
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Der Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

Beispiel

Im folgenden Beispiel werden die Speichersysteme angezeigt, die dem Profil mjullian zugeordnet sind:

```
smo storage list -profile mjullian
```

```
Sample Output:
Storage Controllers
--------------------
FAS3020-RTP07OLD
```

Der Befehl smo Storage umbenennen

Dieser Befehl aktualisiert den Namen oder die IP-Adresse des Speichersystems.

Syntax

```
        smo storage rename
-profile profile
-oldname old_storage_name
-newname new_storage_name
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-oldname old_Storage_Name**

  Gibt die IP-Adresse oder den Namen des Storage-Systems an, bevor das Storage-System umbenannt wird. Sie müssen die IP-Adresse oder den Namen des Speichersystems eingeben, die angezeigt wird, wenn Sie den Befehl smoStorage list ausführen.

- **-newname New_Storage_Name**

  Gibt die IP-Adresse oder den Namen des Storage-Systems nach der Umbenennung des Storage-Systems an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird der Befehl smo Storage umbenennen, um das Speichersystem umzubenennen:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Der SMO System Dump Befehl

Sie können den Systemdump-Befehl ausführen, um eine JAR-Datei zu erstellen, die Diagnoseinformationen zur Serverumgebung enthält.

Syntax

```
        smo system dump
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel des Befehls „System Dump“

Im folgenden Beispiel wird der Befehl smo System dump verwendet, um eine JAR-Datei zu erstellen:

```
smo system dump
Path:/userhomedirectory/.netapp/smo/3.3.0/smo_dump_hostname.jar
```

Der Befehl smo System verify

Dieser Befehl bestätigt, dass alle Komponenten der Umgebung, die zum Ausführen von SnapManager erforderlich sind, ordnungsgemäß eingerichtet werden.

Syntax

```
        smo system verify
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispiel des Befehls „System verify“

Im folgenden Beispiel wird der Befehl smo System verify verwendet.

```
smo system verify
SMO-13505 [INFO ]: Snapdrive verify passed.
SMO-13037 [INFO ]: Successfully completed operation: System Verify
SMO-13049 [INFO ]: Elapsed Time: 0:00:00.559
Operation Id [N4f4e910004b36cfecee74c710de02e44] succeeded.
```

Der Befehl smo Version

Sie können den Versionsbefehl ausführen, um festzulegen, welche Version von SnapManager Sie auf Ihrem lokalen Host ausführen.

Syntax

```
        smo version
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt das Erstellungsdatum und den Inhalt der einzelnen Profile an. Zeigt auch Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel des Versionsbefehls

Im folgenden Beispiel wird die Version des SnapManager angezeigt:

```
smo version
SnapManager for Oracle Version: 3.3.1
```

SnapManager zur Fehlerbehebung

Hier finden Sie Informationen über einige der häufigsten Probleme, die auftreten können, und über deren Behebung.

In der folgenden Tabelle werden häufige Probleme und mögliche Lösungen beschrieben:

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
Werden die Zieldatenbank und der Listener ausgeführt?	Führen Sie den Befehl lsnrctl Status aus. Stellen Sie sicher, dass die Datenbankinstanz beim Listener registriert ist.
Ist der Storage sichtbar?	Führen Sie den befehl SnapDrive Storage show -all aus.
Ist der Storage beschreibbar?	Bearbeiten Sie eine Datei im Bereitstellungspunkt, den Sie gerade erstellt haben. Verwenden Sie den Befehl touch filename. Wenn die Datei erstellt wird, ist Ihr Speicher beschreibbar. Sie müssen sicherstellen, dass der Speicher vom Benutzer beschreibbar ist, auf dem SnapManager ausgeführt wird (z. B. als Root auf UNIX).
Wird der SnapManager Server ausgeführt?	Führen Sie smo_Server Status aus und versuchen Sie, den Server mit dem Befehl smo_Server Start zu starten. Bevor Sie SnapManager-Befehle für Profile mit der grafischen Benutzeroberfläche (GUI) oder der Befehlszeilenschnittstelle (CLI) initiieren können, muss der Server ausgeführt werden. Sie können Repositorys erstellen oder aktualisieren, ohne den Server zu starten. Um jedoch alle anderen SnapManager-Vorgänge auszuführen, muss der Server ausgeführt werden. Geben Sie zum Starten des SnapManager-Servers den folgenden Befehl ein: smo_Server starte.
Sind alle Komponenten erforderlich, um SnapManager korrekt auszuführen?	Führen Sie den smo System verify Befehl aus, um zu überprüfen, dass SnapDrive korrekt eingerichtet ist.
Verfügen Sie über die richtige Version von SnapManager?	Verwenden Sie den Befehl smo Version, um die SnapManager-Version zu überprüfen.

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
Haben Sie sich die Protokolldateien von SnapManager angesehen, um zu ermitteln, ob die Fehlermeldungen helfen können, das Problem zu isolieren?	SnapManager zeichnet alle Log-Einträge in einem Satz rotierender Log-Dateien auf. Die Protokolldateien finden Sie unter /var/log/smo. Die Log-Dateien sind unter C:\Program_Files\NetApp\SnapManager für Oracle\logs zu finden. Es könnte auch hilfreich sein, sich die Protokolle an folgender Stelle anzusehen: /Usr_Home/.netapp/smo/3.3.0/log/ Jedes Betriebsprotokoll wird in seine eigene Protokolldatei der Form smo_of_date_time.log geschrieben.
Wenn auf einem Storage-System, auf dem Data ONTAP nicht ausgeführt wird, Archivprotokolle gespeichert sind, haben Sie diese von Überlegungen für Backups mit SnapManager ausgeschlossen?	Mit der Datei smo.config können Sie bestimmte Archiv-Log-Dateien ausschließen. Für UNIX befinden sich die Dateien an folgender Stelle: /Opt/NetApp/smo/Properties/smo.config Verwenden Sie das in der Datei erwähnte Format, um die lokalen Archivprotokolle auszuschließen. Weitere Informationen finden Sie im Thema „`SBenetzungskonfigurationseigenschaften`“. Sie können die Ziele für das Archivprotokoll auch ausschließen, wenn Sie ein Backup von der SnapManager-CLI erstellen. Weitere Informationen finden Sie im Thema „`Datenbanksicherungen erstellen`“. Sie können die Ziele für das Archivprotokoll auch ausschließen, wenn Sie ein Backup von der SnapManager-GUI erstellen.
Haben Sie eine FlexClone Lizenz, wenn Sie SnapManager mit NFS Datenbanken verwenden?	Zur Nutzung aller Vorteile von SnapManager mit NFS-Datenbanken ist eine FlexClone Lizenz erforderlich. SnapManager erledigt diese Aufgaben mit der FlexClone Funktion: • Backups von NFS-Datenbanken mounten • Backup von NFS-Datenbanken überprüfen • Klonen von NFS-Datenbanken • Registrieren von Backups der NFS-Datenbanken mit RMAN (bei Verwendung von RMAN)

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
Konnte keine Verbindung zum Repository hergestellt werden?	Wenn die Verbindung zu einem Repository fehlschlägt, führen Sie den Befehl lsnrctl Status in der Repository-Datenbank aus, und überprüfen Sie die aktiven Dienstnamen. Wenn SnapManager eine Verbindung zur Repository-Datenbank herstellt, wird der Servicename der Datenbank verwendet. Je nach Einrichtung des Listeners kann dies der kurze Servicename oder der vollqualifizierte Servicename sein. Wenn SnapManager eine Verbindung zu einer Datenbank für einen Backup-, Restore- oder anderen Vorgang herstellt, verwendet er den Host-Namen und den SID. Wenn das Repository nicht korrekt initialisiert wird, weil es derzeit nicht erreichbar ist, erhalten Sie eine Fehlermeldung, in der Sie gefragt werden, ob Sie das Repository entfernen möchten. Sie können das Repository aus Ihrer aktuellen Ansicht entfernen, sodass Sie Vorgänge für andere Repositories ausführen können. Prüfen Sie außerdem, ob die Repository-Instanz ausgeführt wird, indem Sie das ps -eaf ausführen
Grepinstance - Name Befehl.	Kann das System den Hostnamen auflösen?
Überprüfen Sie, ob sich der angegebene Hostname in einem anderen Subnetz befindet. Wenn Sie eine Fehlermeldung erhalten, dass SnapManager den Hostnamen nicht auflösen kann, fügen Sie den Hostnamen in die Hostdatei hinzu.Fügen Sie den Hostnamen zur Datei unter /etc/Hosts hinzu: Xxx.xxx.xxx.xxx.xxx Hostname IP-Adresse	Führt SnapDrive aus?
Überprüfen Sie, ob der SnapDrive Daemon ausgeführt wird: -Snapdrived Status Wenn der Daemon nicht ausgeführt wird, wird eine Meldung angezeigt, die angibt, dass ein Verbindungsfehler vorliegt.	Welche Storage-Systeme sind für den Zugriff mit SnapDrive konfiguriert?
Führen Sie den Befehl: -SnapDrive config list aus	Wie kann die SnapManager GUI Performance verbessert werden?

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
• Stellen Sie sicher, dass Sie über gültige Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil verfügen. Wenn Ihre Anmeldedaten ungültig sind, löschen Sie die Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil. Setzen Sie dieselben Benutzeranmeldeinformationen zurück, die Sie zuvor für das Repository, den Profilhost und das Profil festgelegt haben. Weitere Informationen zum erneuten Einstellen der Benutzeranmeldeinformationen finden Sie unter „`SFestlegen von Anmeldeinformationen nach Löschen des Anmeldeinformationscache`“. • Schließen Sie die nicht verwendeten Profile. Wenn mehr Profile geöffnet werden, wird die Performance der SnapManager GUI beeinträchtigt. • Überprüfen Sie, ob Sie **beim Start öffnen** im Fenster Benutzereinstellungen im Menü **Admin** in der SnapManager-Benutzeroberfläche aktiviert haben. Wenn diese Option aktiviert ist, wird die unter /root/.netapp/smo/3.3.0/gui/State verfügbare Benutzerkonfigurationsdatei (user.config) als openOnStartup=PROFIL angezeigt. Da **Öffnen auf Start** aktiviert ist, müssen Sie nach kürzlich geöffneten Profilen aus der SnapManager-Benutzeroberfläche suchen, wobei lastOpenProfiles in der Benutzerkonfiguration (user.config)-Datei verwendet werden: LASTOPENPROFILE1,PROFILE2,PROFIL3,… Sie können die aufgeführten Profilnamen löschen und immer eine minimale Anzahl von Profilen als offen halten. • Das geschützte Profil benötigt mehr Zeit zur Aktualisierung als das nicht geschützte Profil. Das geschützte Profil wird in einem Zeitintervall aktualisiert, basierend auf dem im protectionStatusRefresRate Parameter der Benutzerkonfigurationsdatei (user.config) angegebenen Wert. Sie können den Wert aus dem Standardwert (300 Sekunden) erhöhen, sodass die geschützten Profile erst nach dem festgelegten Zeitintervall aktualisiert werden.	Wenn mehrere SnapManager Vorgänge gestartet und gleichzeitig im Hintergrund ausgeführt werden, benötigt die SnapManager GUI mehr Zeit für die Aktualisierung. Wenn Sie mit der rechten Maustaste auf das Backup klicken (das bereits gelöscht ist, aber immer noch in der SnapManager GUI angezeigt wird), sind die Backup-Optionen für dieses Backup nicht im Fenster Backup oder Clone aktiviert.

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
Sie müssen warten, bis die SnapManager GUI aktualisiert wird, und dann den Backup-Status überprüfen.	Was würden Sie tun, wenn die Oracle-Datenbank nicht auf Englisch eingestellt ist?
SnapManager-Vorgänge können fehlschlagen, wenn die Sprache für eine Oracle-Datenbank nicht auf Englisch festgelegt ist. Legen Sie die Sprache der Oracle-Datenbank auf Englisch fest: 1. Fügen Sie unter den ersten Kommentaren in /etc/init.d/smo_Server Folgendes hinzu ◦ NLS_LANG=American_America ◦ NLS_LANG exportieren 2. Starten Sie den SnapManager-Server mit dem folgenden Befehl neu: smo_Server restart Wenn die Anmeldeskripte wie .bash_profile, .bashrc und .cschric für den Oracle-Benutzer auf NLS_LANG gesetzt sind, müssen Sie das Skript bearbeiten, um NLS_LANG nicht zu überschreiben.	Was würden Sie tun, wenn die Backup-Planung fehlschlägt, wenn die Repository-Datenbank auf mehr als eine IP verweist und jede IP einen anderen Hostnamen hat?
1. Beenden Sie den SnapManager-Server. 2. Löschen Sie die Zeitplandateien im Repository-Verzeichnis von den Hosts, auf denen Sie den Backup-Zeitplan auslösen möchten. Die Namen der Zeitplandateien können in den folgenden Formaten vorliegen: ◦ Repository#repo_username#Repository_Database_Name#Repository_Host#repo_Port ◦ Repository-repo_usernamerepository_Database_Name-Repository_Host-repo_Port **Hinweis:** Sie müssen sicherstellen, dass Sie die Terminplandatei in dem Format löschen, das den Details des Projektarchivs entspricht. 3. Starten Sie den SnapManager-Server neu. 4. Öffnen Sie andere Profile unter dem gleichen Repository von der SnapManager GUI, um sicherzustellen, dass keine Terminplaninformationen dieser Profile fehlen.	Was würden Sie tun, wenn der SnapManager-Vorgang mit dem Fehler der Dateisperre für Zugangsdaten fehlschlägt?

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
SnapManager sperrt die Anmeldeinformationsdatei vor dem Aktualisieren und entsperrt sie nach dem Aktualisieren.Wenn mehrere Operationen gleichzeitig ausgeführt werden, kann einer der Operationen die Anmeldeinformationsdatei sperren, um sie zu aktualisieren. Wenn ein anderer Vorgang versucht, gleichzeitig auf die Datei mit gesperrten Anmeldeinformationen zuzugreifen, schlägt der Vorgang mit dem Dateisperrfehler fehl. Konfigurieren Sie in der Datei smo.config die folgenden Parameter, je nach Häufigkeit der gleichzeitigen Operationen: • FileLock.retryIntervall = 100 Millisekunden • FileLock.Timeout = 5000 Millisekunden Die den Parametern zugewiesenen Werte müssen in Millisekunden liegen.	Was würden Sie tun, wenn der Zwischenstatus des Backup Verify-Vorgangs auf der Registerkarte Monitor fehlgeschlagen angezeigt wird, obwohl der Backup Verify-Vorgang noch ausgeführt wird?
Die Fehlermeldung wird in der Datei sm_gui.log protokolliert. Sie müssen in der Protokolldatei nachsehen, um die neuen Werte für den Vorgang zu bestimmen.heartbeatIntervall und Operation.heartbeatThreshold Parameter, die dieses Problem lösen werden. 1. Fügen Sie die folgenden Parameter in der Datei smo.config hinzu: ◦ Operation.heartbeatIntervall = 5000 ◦ Operation.heartbeatThreshold = 5000 der von SnapManager zugewiesene Standardwert ist 5000. 2. Diesen Parametern die neuen Werte zuweisen. Die den Parametern zugewiesenen Werte müssen in Millisekunden liegen. 3. Starten Sie den SnapManager-Server neu, und führen Sie den Vorgang erneut aus.	Was ist zu tun, wenn ein Heap-Space-Problem auftritt?

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung
Wenn während des SnapManager für Oracle-Betriebs ein Heap-Space-Problem auftritt, müssen Sie die folgenden Schritte durchführen: 1. Wechseln Sie zum Installationsverzeichnis für SnapManager für Oracle. 2. Öffnen Sie die Datei launchjava aus dem Installationsverzeichnis/bin/launchjava-Pfad. 3. Erhöhen Sie den Wert des Java -Xmx160m Java Heap-space Parameters. So können Sie beispielsweise den Standardwert von 160 m auf 200 m erhöhen. Wenn Sie den Wert des Java Heap-space-Parameters in den früheren Versionen von SnapManager für Oracle erhöht haben, sollten Sie diesen Wert beibehalten.	Was würden Sie tun, wenn Sie die geschützten Backups nicht zum Wiederherstellen oder Klonen verwenden können?
Dieses Problem wird beobachtet, wenn Sie SnapManager 3.3.1 mit Clustered Data ONTAP verwendet haben und ein Upgrade auf SnapManager 3.4 durchgeführt haben. Die Backups wurden mithilfe von Post-Skripten in SnapManager 3.3 gesichert. Ab SnapManager 3.4 sind die Backups entweder über *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* Richtlinien gesichert, die beim Erstellen eines Profils ausgewählt werden. Nach einem Upgrade auf SnapManager 3.4 können Sie eventuell noch die alten Profile nutzen und so Backups mit Backup-Skripten schützen. Sie können sie aber nicht zur Wiederherstellung oder zum Klonen mit SnapManager verwenden. Sie müssen das Profil aktualisieren und entweder die Richtlinie *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* auswählen und das Post-Skript, das zur Datensicherung in SnapManager 3.3 verwendet wurde, löschen.	Was würden Sie tun, wenn geplante Backups nicht gesichert werden (SnapVault)?

Speicherauszug-Dateien

Die Dump-Dateien sind komprimierte Log-Dateien, die Informationen über SnapManager und seine Umgebung enthalten. Die verschiedenen Typen von erstellten Log-Dateien sind Operation, Profil und System-Dump-Datei.

Sie können den Dump-Befehl oder die Registerkarte **Create Diagnostics** in der grafischen Benutzeroberfläche (GUI) verwenden, um Informationen über einen Vorgang, ein Profil oder die Umgebung zu sammeln. Ein System-Dump erfordert kein Profil. Das Profil und die Operation Dumps erfordern jedoch Profile.

SnapManager enthält die folgenden Diagnoseinformationen in der Dump-Datei:

- Die durchgeführten Schritte
- Die Zeitdauer für jeden Schritt
- Das Ergebnis jedes Schritts
- Fehler, falls vorhanden, der während des Vorgangs aufgetreten ist

SnapManager-Protokolldateien oder Dump-Dateien ermöglichen Lese- und Schreibberechtigungen nur für die Root-Benutzer und die anderen Benutzer, die zur Root-Benutzergruppe gehören.

SnapManager enthält auch die folgenden Informationen in der Datei:

- Version und Architektur des Betriebssystems
- Umgebungsvariablen
- Java-Version
- SnapManager Version und Architektur
- SnapManager-Einstellungen
- SnapManager Nachrichten
- Eigenschaften log4j
- SnapDrive Version und Architektur
- SnapDrive-Protokolldateien
- Oracle Version
- Oracle Owatch – Details zum lokalen Bestand
- Die automatische Speicherverwaltung (ASM)-Instanz ermöglicht die automatische Verriegelung lokaler Bestandsdaten
- Version des Storage-Systems
- Oracle oratab-Datei
- Oracle-Listener-Status
- Oracle Netzwerkkonfigurationsdateien (Listener.ora und ntsnames.ora)
- Oracle Version der Repository-Datenbank
- Typ der Zieldatenbank (Stand-Aloneor Real Application Clusters (RAC))
- Zieldatenbankrolle (primärer, physischer Standby oder logischer Standby)
- Einrichtung der Zieldatenbank Oracle Recovery Manager (RMAN) (keine RMAN Integration, RMAN mit Kontrolldateien oder RMAN mit Katalogdatei)
- ASM-Instanzversion der Zieldatenbank
- Oracle Version der Zieldatenbank
- System Identifier (SID) der Zieldatenbank

- RMAN-Datenbankname und TNS-Verbindungsname
- Name des Repository-Datenbankdienstes
- Auf dem Host installierte Datenbankinstanzen
- Profildeskriptor
- Maximaler gemeinsam genutzter Speicher
- Swap-Informationen zum Speicherplatz
- Speicherinformationen
- Kernel-Version
- FSTAB
- Von SnapDrive verwendetes Protokoll
- Multipath-Umgebung
- RAC
- Unterstützter Volume Manager
- Version von Operations Manager
- Unterstütztes Dateisystem
- Host Utilities-Version
- Ausgabe des Befehls „System Verify“
- Ausgabe des sdconfcheck-Befehls

SnapManager Dump-Dateien enthalten auch die SnapDrive Datensammler-Datei und die Oracle Alert Log-Datei. Sie können die Oracle Alert Log-Datei unter Verwendung der SMO Operation Dump und smo profile dump Befehle sammeln.

System Dump enthält keine Oracle-Alarmprotokolle. Das Profil und die Operation Dumps enthalten jedoch die Alarmprotokolle.

Selbst wenn der SnapManager Host Server nicht ausgeführt wird, können Sie über die Befehlszeilenschnittstelle (CLI) oder die GUI auf die Dump-Informationen zugreifen.

Wenn ein Problem auftritt, das nicht gelöst werden kann, können Sie diese Dateien an NetApp Global Services senden.

Erstellen von Dump-Dateien auf Betriebsebene

Sie können den Befehl smo Operation dump mit dem Namen oder der ID des fehlgeschlagenen Vorgangs verwenden, um Protokollinformationen über einen bestimmten Vorgang zu erhalten. Sie können unterschiedliche Protokollebenen festlegen, um Informationen zu einem bestimmten Vorgang, Profil, Host oder einer bestimmten Umgebung zu erfassen.

1. Geben Sie den folgenden Befehl ein:Smo Operation dump -idguid

Der smo Operation dump Befehl stellt einen super Satz der Informationen zur Verfügung, die vom smo profile dump Befehl bereitgestellt werden, was wiederum einen super Satz von den Informationen bietet, die vom smo System dump Befehl zur Verfügung gestellt werden.

Speicherverzeichnis der Speicherdatei:

```
Path:/<user-home>
/.netapp/smo/3.3.0/smo_dump_8abc01c814649ebd0114649ec69d0001.jar
```

Erstellen von Dump-Dateien auf Profilebene

Mithilfe des Befehls smo profile dump mit dem Namen des Profils können Sie Protokollinformationen zu einem bestimmten Profil finden.

1. Geben Sie den folgenden Befehl ein: smo profile dump -profile Profile_Name

   Speicherverzeichnis der Speicherdatei:

   ```
   Path:/<user-home>
   /.netapp/smo/3.3.0/smo_dump_8abc01c814649ebd0114649ec69d0001.jar
   ```

   Wenn beim Erstellen eines Profils ein Fehler auftritt, verwenden Sie den Befehl „Smosystem dump“. Nachdem Sie ein Profil erfolgreich erstellt haben, verwenden Sie die Befehle SmoOperation dump und scoprofile dump.

Erstellen von Dump-Dateien auf Systemebene

Sie können den smo System Dump Befehl verwenden, um Protokollinformationen über den SnapManager Host und die Umgebung zu erhalten. Sie können unterschiedliche Protokollebenen angeben, um Informationen zu einem bestimmten Vorgang, Profil oder Host und Umgebung zu erfassen.

1. Geben Sie den folgenden Befehl ein: smo System Dump

   Daraus resultierender Dump

   ```
   Path:/<user-home>/.netapp/smo/3.3.0/smo_dump_server_host.jar
   ```

So finden Sie Speicherauszugsdateien

Die Dump-Datei befindet sich im Client-System für einfachen Zugriff. Diese Dateien sind hilfreich, wenn Sie Probleme im Zusammenhang mit Profil, System oder einer beliebigen Operation beheben müssen.

Die Dump-Datei befindet sich im Home-Verzeichnis des Benutzers auf dem Client-System.

- Wenn Sie die grafische Benutzeroberfläche (GUI) verwenden, befindet sich die Dump-Datei unter:

```
user_home/Application Data/NetApp/smo/3.3.0/smo_dump dump_file_type_name
server_host.jar
```

- Wenn Sie die Befehlszeilenschnittstelle (CLI) verwenden, befindet sich die Dump-Datei unter:

```
user_home/.netapp/smo/3.3.0/smo_dump_dump_file_type_name server_host.jar
```

Die Dump-Datei enthält die Ausgabe des Dump-Befehls. Der Name der Datei hängt von den angegebenen Informationen ab. In der folgenden Tabelle werden die Typen von Dump-Operationen und die daraus resultierenden Dateinamen angezeigt:

Typ des Speicherauszugsvorgangs	Dateiname wird angezeigt
Befehl für den Operation Dump mit Vorgangs-ID	smo_dump_operation-id.jar

Der Befehl für den Operation Dump enthält keine Vorgangs-ID	smo Operation Dump -Profile VH1-verbose die folgende Ausgabe wird angezeigt:
	`smo operation dump -profile VH1 -verbose`
	`[ INFO] SMO-13048: Dump Operation Status: SUCCESS`
	`[ INFO] SMO-13049: Elapsed Time: 0:00:01.404`
	`Dump file created.`
	`Path: /oracle/VH1/<path>/smo/3.3.0/smo_dump_VH1_kaw.rtp.foo.com.jar`

Befehl für System Dump	smo_dump_host-name.jar
Profildump-Befehl	smo_dump_profile-name_host-name.jar

So sammeln Sie Speicherauszugsdateien

Sie können -dump in den SnapManager-Befehl einschließen, um die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen SnapManager-Vorgang zu sammeln.

Sie können Dump-Dateien für die folgenden SnapManager-Vorgänge sammeln:

- Profile werden erstellt
- Profile werden aktualisiert
- Backups werden erstellt
- Backups werden überprüft
- Backups werden gelöscht
- So werden Backups entlastet
- Montage von Backups
- UnMounten von Backups
- Backups werden wiederhergestellt
- Klone werden erstellt
- Klone werden gelöscht
- Aufteilung von Klonen

Wenn Sie ein Profil erstellen, können Sie Dump-Dateien nur sammeln, wenn der Vorgang erfolgreich ist. Wenn beim Erstellen eines Profils ein Fehler auftritt, müssen Sie den Befehl „Smosystem dump“ verwenden. Für erfolgreiche Profile können Sie die SmoOperation Dump und smoprofile Dump-Befehle verwenden, um die Dump-Dateien zu sammeln.

Beispiel

```
      smo  backup create -profile targetdb1_prof1 -auto -full -online
-dump
```

Sammeln zusätzlicher Protokollinformationen für eine einfachere Fehlersuche

Wenn Sie zusätzliche Protokolle benötigen, um einen fehlgeschlagenen SnapManager-Vorgang zu debuggen, müssen Sie eine externe Umgebungsvariable Server.log.Level festlegen. Diese Variable überschreibt die Standard-Protokollebene und lädt alle Protokollmeldungen in der Protokolldatei ab. Sie können beispielsweise die Protokollebene in DEBUG ändern, die zusätzliche Meldungen protokolliert und beim Debuggen von Problemen helfen kann.

Die SnapManager-Protokolle sind an folgenden Orten zu finden:

- /Var/log/smo

Um die Standard-Protokollebene außer Kraft zu setzen, müssen Sie die folgenden Schritte durchführen:

1. Erstellen Sie eine Platform.override-Textdatei im SnapManager-Installationsverzeichnis.
2. Fügen Sie den Parameter Server.log.Level in die Textdatei Platform.override ein.
3. Weisen Sie einen Wert zu (TRACE, DEBUG, INFO, WARN, ERROR, FATAL oder PROGRESS) zum Parameter Server.log.Level.

   Um z. B. die Protokollebene auf FEHLER zu ändern, setzen Sie den Wert von Server.log.Level auf FEHLER.

Server.log.Level=FEHLER

4. Starten Sie den SnapManager-Server neu.

Wenn keine zusätzlichen Protokollinformationen erforderlich sind, können Sie den Parameter Server.log.Level aus der Textdatei Platform.override löschen.

SnapManager verwaltet die Menge der Server-Log-Dateien auf der Grundlage der benutzerdefinierten Werte der folgenden Parameter in der Datei smo.config:

- Log.max_log_files
- Log.max_log_file_size
- Log.max_Rolling_Operation_Factory_logs

Fehlerbehebung bei Klonproblemen

Hier finden Sie Informationen darüber, die während eines Klonens auftreten können und wie Sie sie lösen können.

Symptom	Erklärung	Behelfslösung
Der Klonvorgang schlägt fehl, wenn das Archivziel auf USE_DB_RECOVERY_FILE_DEST gesetzt ist.	Wenn sich das Archivziel auf USE_DB_RECOVERY_FILE_DEST bezieht, verwaltet der Flash Recovery Area (FRA) aktiv das Archivprotokoll. SnapManager nutzt den FRA-Standort nicht während Klon- oder Restore-Vorgängen und schlägt somit fehl.	Ändern Sie das Archivziel in den tatsächlichen Speicherort des Archivprotokolls anstelle des FRA-Speicherorts.

Symptom	Erklärung	Behelfslösung
Der Klonvorgang schlägt mit der folgenden Fehlermeldung fehl: Der Vorgang kann nicht ausgeführt werden: Clone Create. Ursache: ORACLE-00001: Fehler beim Ausführen von SQL: [DATENBANK ÄNDERN ÖFFNEN RESETLOGS;]. Der Befehl zurückgegeben: ORA-01195: Online Backup der Datei 1 benötigt mehr Wiederherstellung, um konsistent zu sein.	Dieses Problem tritt auf, wenn Oracle Listener die Verbindung zur Datenbank nicht herstellen kann.	Wenn Sie ein Backup mit der GUI von SnapManager klonen, führen Sie die folgenden Aktionen durch: 1. Klicken Sie im Repository-Baum auf **Repository** > **Host** > **Profil**, um die Backups anzuzeigen. 2. Klicken Sie mit der rechten Maustaste auf das Backup, das Sie klonen möchten, und wählen Sie **Clone** aus. 3. Geben Sie auf der Seite Clone Initialization die obligatorischen Werte ein, und wählen Sie die Methode Clone Specification aus. 4. Wählen Sie auf der Seite „Spezifikation klonen“ die Option **Parameter** aus. 5. Klicken Sie auf die Registerkarte **+Parameter**. 6. Geben Sie im Feld **Parametername** den Namen als local_Listener ein und klicken Sie auf **OK**. 7. Aktivieren Sie das Kontrollkästchen **Standard überschreiben** für die Zeile Local_Listener. 8. Klicken Sie auf einen beliebigen Parameter, doppelklicken Sie dann auf den Parameter Local_Listener, und geben Sie den folgenden Wert ein:(ADDRESS=(PROTOCOL=TCP)(HOST=<your_Host_Name>)(PORT=<Port#>)) 9. Klicken Sie Auf **In Datei Speichern**. 10. Klicken Sie auf **Weiter** und fahren Sie mit dem Clone create Wizard fort. Wenn Sie ein Backup über CLI klonen, müssen Sie die folgenden Informationen in das Tag **<Parameter>** der Klon-Spezifikations-Datei einfügen:

Symptom	Erklärung	Behelfslösung
Der Klonvorgang schlägt mit einer Fehlermeldung fehl, die sagt, dass der von Ihnen verwendete Mountpoint bereits verwendet ist.	Mit SnapManager können Sie einen Klon nicht über einem bestehenden Bereitstellungspunkt mounten. Ein unvollständiger Klon hat den Bereitstellungspunkt nicht entfernt.	Geben Sie einen anderen Bereitstellungspunkt an, der vom Klon verwendet werden soll, oder heben Sie den problematischen Bereitstellungspunkt auf.
Der Klonvorgang schlägt fehl mit einer Fehlermeldung, dass Datendateien keine .dbf-Erweiterung haben.	Einige Versionen des Oracle NID-Dienstprogramms funktionieren nicht mit Datendateien, es sei denn, die Dateien verwenden eine .dbf-Erweiterung.	• Benennen Sie die Datendatei um, um eine .dbf-Erweiterung zu erhalten. • Wiederholen Sie den Sicherungsvorgang. • Klonen des neuen Backups:
Aufgrund der nicht erfüllten Anforderungen schlägt der Klonvorgang fehl.	Sie versuchen, einen Klon zu erstellen. Einige der Voraussetzungen wurden jedoch nicht erfüllt.	Fahren Sie wie unter *Erstellen eines Klons* beschrieben fort, um die Voraussetzungen zu erfüllen.
Nach dem Aufteilen des Klons kann SnapManager kein neues Profil generieren, und der Benutzer weiß nicht, ob das neue Profil erstellt wird.	SnapManager kann nicht aufgefordert werden, wenn ein neues Profil nach dem Split-Vorgang des Klons nicht erstellt wird. Da die Eingabeaufforderung nicht angezeigt wird, können Sie davon ausgehen, dass das Profil erstellt wird.	Geben Sie in der Befehlszeilenschnittstelle (CLI) von SnapManager den Befehl Clone Split-Ergebnis ein, um das detaillierte Ergebnis des Klonteilvorgangs anzuzeigen.
SnapManager für Oracle klont keine physischen Oracle Data Guard Standby Datenbanken (10.2.0.5).	SnapManager für Oracle deaktiviert den verwalteten Recovery-Modus nicht, während ein Offline-Backup der physischen Oracle 10gR2 (10.2.0.5) Standby-Datenbanken durchgeführt wird, die mit Oracle Data Guard Services erstellt wurden. Aufgrund dieses Problems ist das Offline Backup inkonsistent. Wenn SnapManager für Oracle versucht, das Offline-Backup zu klonen, wird nicht einmal versucht, eine Wiederherstellung auf der geklonten Datenbank durchzuführen. Da das Backup inkonsistent ist, muss die geklonte Datenbank wiederhergestellt werden, und damit kann Oracle den Klon nicht erfolgreich erstellen.	Aktualisieren Sie die Oracle-Datenbank auf Oracle 11gR1 (Patch 11.1.0.7).

Symptom	Erklärung	Behelfslösung
Das Klonen einer Sicherung auf einen Remote-Host schlägt mit der folgenden Fehlermeldung fehl Fehler: Der Zugriff wird verweigert.	Wenn im Mounten die IP-Adresse des Hosts dem Befehl Snap Mount bereitgestellt wird, kann der Klonvorgang fehlschlagen. Dieses Problem tritt auf, wenn sich der Host, auf dem sich die Datenbank befindet, in der Arbeitsgruppe befindet, während sich der Remote-Host in der Domäne befindet, oder umgekehrt.	Sie müssen sicherstellen, dass sich sowohl der Remote-Host als auch der Host, auf dem sich die Datenbank befindet, in der Domäne und nicht in der Arbeitsgruppe befinden.

Fehlerbehebung bei Problemen mit der grafischen Benutzeroberfläche

Sie finden Informationen zu einigen Problemen der grafischen Benutzeroberfläche (GUI), die Ihnen bei der Problembehebung helfen könnten.

Problem	Erklärung	Behelfslösung
Beim Zugriff auf die SnapManager-Benutzeroberfläche zur Durchführung eines Vorgangs kann die folgende Fehlermeldung angezeigt werden: SMO-20111 : Authentifizierung für Benutzer auf dem Host fehlgeschlagen.	Dieses Problem tritt auf, wenn das Kennwort des Benutzers in dem Host geändert wird, auf dem der SnapManager-Server ausgeführt wird.Nachdem das Passwort geändert wurde, wird der Anmeldeinformationscache, der für den Benutzer erstellt wird, der die GUI gestartet hat, ungültig. Die SnapManager-GUI verwendet zur Authentifizierung weiterhin die Zugangsdaten im Cache und schlägt somit fehl.	Sie müssen eine der folgenden Aufgaben durchführen: • Löschen Sie die Anmeldeinformationen des Benutzers, dessen Passwort geändert wurde, und fügen Sie dann die neuen Anmeldeinformationen in den Cache ein, indem Sie die folgenden Befehle ausführen: a. löschen von smo-Anmeldeinformationen b. smo Credentials-Satz • Löschen Sie den gesamten Cache, indem Sie den Befehl smo centimals clear ausführen. Öffnen Sie die GUI erneut, und legen Sie die Anmeldeinformationen fest, falls Sie dazu aufgefordert werden.

Problem	Erklärung	Behelfslösung
Die Sicherheitswarnung wird angezeigt, wenn Sie Java Web Start verwenden, um auf die SnapManager-GUI zuzugreifen.	Beim Zugriff auf die SnapManager-GUI mit Java Web Start wird eine Sicherheitswarnung angezeigt.Dieses Problem tritt auf, weil JNLP-JARs selbstsigniert sind und die von SnapManager verwendete Java-Version keine selbstsignierten Jars auf hoher Sicherheitsstufe zulässt.	Ändern Sie entweder die Sicherheitseinstellungen im java-Bedienfeld auf Medium, oder fügen Sie die SnapManager-GUI-URL zur Ausnahmeliste hinzu.
In der SnapManager Webstart-GUI wird die falsche Version angezeigt.	Nachdem Sie beim Start der Web-Start-GUI die SnapManager von einer neueren Version auf eine frühere Version heruntergestuft haben, wird die neuere Version der SnapManager Web-Start-GUI gestartet.	Sie müssen den Cache auch löschen, indem Sie die folgenden Schritte durchführen: 1. Starten Sie die Konsole. 2. Geben Sie Folgendes ein: Javaws -Viewer 3. Klicken Sie im Java Cache Viewer-Bildschirm mit der rechten Maustaste auf die SnapManager-Anwendung und wählen Sie **Löschen** aus.
Wenn Sie die GUI neu starten und versuchen, die Backups auf ein bestimmtes Profil zu überprüfen, werden nur die Namen der Profile angezeigt.	SnapManager zeigt erst Informationen zu einem Profil an, wenn Sie es öffnen.	Führen Sie folgende Schritte aus: 1. Klicken Sie mit der rechten Maustaste auf das Profil und wählen Sie im Menü * Öffnen* aus. SnapManager zeigt das Dialogfeld Profilauthentifizierung an. 2. Geben Sie den Benutzernamen und das Kennwort des Hosts ein. SnapManager zeigt die Sicherungsliste an. Sie müssen das Profil nur einmal authentifizieren, solange die Anmeldeinformation en gültig sind und im Cache verbleiben.

Problem	Erklärung	Behelfslösung
Wenn Sie das erste Repository in der GUI öffnen, wird eine Fehlermeldung wie die folgende angezeigt: Der Profilname XXXX wird mit dem zuvor geladenen Repository übereinander.	Identisch benannte Profile können nicht in einem Repository vorhanden sein. Sie können auch nur ein Repository gleichzeitig öffnen.	Verwenden Sie die widersprüchlichen Profile von zwei verschiedenen Betriebssystembenutzern oder benennen Sie das Profil um, indem Sie eine SQL-Anweisung für das Repository ausgeben: AKTUALISIEREN Sie SMO_33_PROFILE SET NAME = 'NEW_NAME' MIT DEM NAMEN = 'OLD_NAME'.
Eine Fehlermeldung ähnlich der folgenden wird angezeigt: SMO-01092: Repository kann nicht initialisiert werden repo1@ existiert nicht:repo1SMO-11006: Der Host kann nicht aufgelöst werden	Das Repository ist unzugänglich, vielleicht weil es nicht mehr existiert. Die GUI initialisiert die Liste der Repositorys aus der Anmeldedatei.	In der Fehlermeldung wird gefragt, ob Sie dieses Repository entfernen möchten, damit kein Versuch unternommen wird, es in der Zukunft zu laden. Wenn Sie nicht auf dieses Repository zugreifen müssen, klicken Sie auf **Löschen**, um es aus der GUI-Ansicht zu entfernen. Dadurch wird der Verweis auf das Repository in der Anmeldedatei entfernt, und die GUI versucht nicht, das Repository erneut zu laden.

Problem	Erklärung	Behelfslösung

Die Profilerstellung schlägt fehl, da die Hostanmeldeinformationen in den Plattformen SUSE Linux Enterprise Server 10 und SUSE Linux Enterprise Server 11 nicht authentifiziert werden.	SnapManager verwendet zur Authentifizierung von Benutzern das Pluggable Authentication Module (PAM). Auf den SUSE Linux Enterprise Server-Plattformen 10 und 11 gibt es im Verzeichnis /etc/pam.d standardmäßig keine SnapManager-Datei, die die erforderlichen Authentifizierungsdetails enthält. Daher schlagen die Host-Anmeldedaten fehl.	So melden Sie sich auf den SUSE Linux Enterprise Server 10- und 11-Plattformen erfolgreich am Host an:
		1. erstellen Sie eine SnapManager-Datei in /etc/pam.d/.
		2. Fügen Sie den folgenden Inhalt zur datei SnapManager unter /etc/pam.d/snapmanager hinzu:
		`#%PAM-1.0`
		`auth include common-auth`
		`account include common-account`
		`password include common-password`
		`session include common-session`
		3. Speichern Sie die Datei, und versuchen Sie es erneut, die Profilerstellung zu erstellen.

SnapManager benötigt eine längere Zeit, um die Baumstruktur der Datenbank zu laden, und führt dazu, dass auf der SnapManager-Benutzeroberfläche eine Fehlermeldung mit einem Timeout angezeigt wird.	Wenn Sie versuchen, einen Teil-Backup-Vorgang von der SnapManager-Benutzeroberfläche auszuführen, versucht SnapManager, die Anmeldeinformationen für alle Profile zu laden. Wenn ungültige Einträge vorliegen, versucht SnapManager, den Eintrag zu validieren. Dies führt dazu, dass eine Fehlermeldung mit einem Timeout angezeigt wird.	Löschen Sie die Anmeldeinformationen des nicht verwendeten Hosts, Repositorys und Profils, indem Sie den Befehl zum Löschen von Anmeldeinformationen in der SnapManager-Befehlszeilenschnittstelle (CLI) verwenden.

Problem	Erklärung	Behelfslösung
Nach der Teilung des Klons kann SnapManager kein neues Profil generieren, und Sie wissen nicht, ob das neue Profil erstellt wird.	SnapManager fordert Sie nicht auf, wenn ein neues Profil nach dem Split-Vorgang des Klons nicht erstellt wird. Da für den fehlgeschlagenen Vorgang keine Meldung angezeigt wird, gehen Sie möglicherweise davon aus, dass das Profil erstellt wird.	Um zu wissen, ob ein neues Profil für den Klon-Split-Vorgang erstellt wird, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf die Registerkarte **Monitor**, klicken Sie mit der rechten Maustaste auf den Eintrag Clone Split Operation und wählen Sie **Eigenschaften**. 2. Klicken Sie im Fenster Profileigenschaften auf die Registerkarte **Protokolle**, um die Protokolle für die Klonteiloperation und die Profilerstellung anzuzeigen.
Die benutzerdefinierten Skripte, die für die vor- oder Nachbearbeitungsaktivität vor oder nach dem Backup-, Restore- oder Klonvorgang ausgeführt werden, sind in der SnapManager GUI nicht sichtbar.	Wenn Sie nach dem Start des jeweiligen Assistenten benutzerdefinierte Skripts in den benutzerdefinierten Speicherort für Backup, Wiederherstellung oder Klonen hinzufügen, werden die benutzerdefinierten Skripts nicht unter der Liste Verfügbare Skripts angezeigt.	Starten Sie den SnapManager-Hostserver neu, und öffnen Sie dann die SnapManager-GUI.
Sie können die in SnapManager (3.1 oder früher) erstellte XML-Datei für die Klonspezifikation nicht verwenden.	Ab SnapManager 3.2 für Oracle wird der Abschnitt Aufgabenspezifikation (Task-Specification) als separate XML-Datei für die Aufgabenspezifikation bereitgestellt.	Wenn Sie SnapManager 3.2 für Oracle verwenden, müssen Sie den Abschnitt für die Aufgabenspezifikation aus der XML für die Klonspezifikation entfernen oder eine neue XML-Datei für die Klonspezifikation erstellen. SnapManager 3.3 oder höher unterstützt nicht die XML-Datei für die Klonspezifikation, die in SnapManager 3.2 oder älteren Versionen erstellt wurde.

Problem	Erklärung	Behelfslösung
Die SnapManager-Operation auf der Benutzeroberfläche wird nicht fortgesetzt, nachdem Sie die Benutzeranmeldeinformationen gelöscht haben, indem Sie den Befehl smo cumm clear von der SnapManager CLI verwenden oder durch Klicken auf **Admin** > **Anmeldeinformationen** > **Löschen** > **Cache** in der SnapManager-Benutzeroberfläche.	Die für Repositorys, Hosts und Profile festgelegten Anmeldeinformationen werden gelöscht. SnapManager überprüft vor dem Starten eines Vorgangs die Benutzeranmeldeinformationen.Wenn die Benutzeranmeldeinformationen ungültig sind, kann sich SnapManager nicht authentifizieren. Wenn ein Host oder ein Profil aus dem Repository gelöscht wird, sind die Benutzeranmeldeinformationen weiterhin im Cache verfügbar. Diese unnötigen Einträge mit Anmeldeinformationen verlangsamen die SnapManager-Vorgänge von der GUI.	Starten Sie die SnapManager GUI neu, je nachdem, wie der Cache gelöscht wird. **Hinweis:** • Wenn Sie den Anmeldeinformationscache von der SnapManager-GUI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche nicht beenden. • Wenn Sie den Anmeldeinformationscache über die SnapManager-CLI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche neu starten. • Wenn Sie die verschlüsselte Anmeldedatei manuell gelöscht haben, müssen Sie die SnapManager-GUI neu starten. Legen Sie die Anmeldeinformationen fest, die Sie für das Repository, den Profilhost und das Profil angegeben haben. Wenn in der SnapManager-GUI kein Repository unter der Struktur Repositories zugeordnet ist, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf **Aufgaben** > **vorhandenes Repository hinzufügen** 2. Klicken Sie mit der rechten Maustaste auf das Repository, klicken Sie auf **Öffnen** und geben Sie die Benutzeranmeldeinformationen im Fenster * Repository Credentials Authentication* ein. 3. Klicken Sie mit der rechten Maustaste auf den Host im Repository, klicken Sie auf **Öffnen** und geben Sie die Benutzeranmeldeinformationen in **Host Authentication** ein. 4. Klicken Sie mit der rechten Maustaste auf das Profil unter dem Host, klicken Sie auf **Öffnen** und geben Sie die Benutzeranmeldeinformationen in **Profilauthentifizierung** ein.

Problem	Erklärung	Behelfslösung
Die Fehlermeldung kann die Schutzrichtlinien aus folgendem Grund nicht auflisten: Der Protection Manager ist vorübergehend nicht verfügbar, wird angezeigt, wenn Sie im Dropdown-Menü **Protection Manager Protection Policy** des Fensters Profileigenschaften und der Seite mit den Richtlinieneinstellungen des Assistenten Profile create **Keine** auswählen.	Der Protection Manager ist nicht mit SnapManager konfiguriert, oder der Protection Manager wird nicht ausgeführt.	Es ist keine Aktion erforderlich.
Sie können die SnapManager-Benutzeroberfläche nicht über die Java Web Start GUI öffnen, da die SSL-Verschlüsselung (Secure Sockets Layer) des Browsers schwächer ist.	SnapManager unterstützt keine SSL-Chiffren, die schwächer als 128 Bit sind.	Aktualisieren Sie die Browserversion und überprüfen Sie die Verschlüsselungsstärke.

Fehlerbehebung bei SnapDrive-Problemen

Es gibt einige häufige Probleme, auf die Sie bei der Verwendung von SnapManager mit SnapDrive Produkten laufen könnten.

Zunächst müssen Sie feststellen, ob das Problem mit SnapManager für Oracle oder SnapDrive zusammenhängt. Wenn das Problem ein SnapDrive-Fehler ist, gibt SnapManager für Oracle eine Fehlermeldung ähnlich wie:

```
SMO-12111: Error executing snapdrive command "<snapdrive command>":
<snapdrive error>
```

Im Folgenden finden Sie ein Beispiel für eine Fehlermeldung von SnapDrive, bei der SMO-12111 die Fehlernummer des SnapManager lautet. Das Nummerierungsschema für 0001-770 stellt SnapDrive für UNIX-Fehler dar.

```
SMO-12111: Error executing snapdrive command
"/usr/sbin/snapdrive snap restore -file
/mnt/pathname/ar_anzio_name_10gR2_arrac1/data/undotbs02.dbf
-snapname pathname.company.com:
/vol/ar_anzio_name_10gR2_arrac1:
TEST_ARRAC1_YORKTOW_arrac12_F_C_0_8abc01b20f9ec03d010f9ec06bee0001_0":
0001-770
Admin error: Inconsistent number of files returned when listing contents
of
/vol/ar_anzio_name_10gR2_arrac1/.snapshot/
TEST_ARRAC1_YORKTOW_arrac12_F_C_0_8abc01b20f9ec03d010f9ec06bee0001_0/data
on filer pathname.
```

Im Folgenden finden Sie die häufigsten Fehlermeldungen von SnapDrive für UNIX in Bezug auf LUN-Erkennung, Konfigurationsprobleme und Speicherplatz. Wenn Sie einen dieser Fehler erhalten, lesen Sie das Kapitel Fehlerbehebung im Installationshandbuch für *SnapDrive*.

Symptom	Erklärung
0001-136 Admin-Fehler: Anmeldung beim Filer nicht möglich: <Filer> Bitte legen Sie den Benutzernamen und/oder das Passwort für <Filer> fest	Erstkonfiguration von SnapDrive
0001-382 Admin-Fehler: Multipathing-Rescan fehlgeschlagen	Fehler bei der LUN-Erkennung
0001-462 Admin-Fehler: Konnte Multipathing für <LUN> nicht aufheben: Spd5: Gerät kann nicht angehalten werden. Gerät belegt.	Fehler bei der LUN-Erkennung
0001-476 Admin error: Das Gerät, das mit dem … 0001-710 Admin-Fehler: OS-Aktualisierung der LUN fehlgeschlagen …	Fehler bei der LUN-Erkennung
0001-680 Admin-Fehler: Host OS erfordert ein Update auf interne Daten, um LUN-Erstellung oder Verbindung zu ermöglichen. Verwenden Sie 'SnapDrive config luns vorbereiten' oder aktualisieren Sie diese Informationen manuell…	Fehler bei der LUN-Erkennung
0001-817 Admin error: Konnte Volume Clone nicht erstellen … : FlexClone nicht lizenziert	Erstkonfiguration von SnapDrive
0001-878 Admin-Fehler: HBA-Assistent wurde nicht gefunden. Befehle, die LUNs betreffen, sollten fehlschlagen.	Fehler bei der LUN-Erkennung

Fehlerbehebung bei der Umbenennung des Speichersystems

Möglicherweise treten Probleme auf, wenn Sie ein Storage-System umbenennen oder das Storage-System erfolgreich umbenannt haben.

Wenn Sie versuchen, das Speichersystem umzubenennen, schlägt der Vorgang möglicherweise mit der folgenden Fehlermeldung fehl: SMO-05085 kein Speicher-Controller „fas3020-rtp07New“ wurde gefunden, der dem Profil zugeordnet ist

Sie müssen die IP-Adresse oder den Namen des Speichersystems eingeben, das aufgelistet ist, wenn Sie den Befehl smoStorage list ausführen.

Nachdem Sie das Storage-System umbenannt haben, können SnapManager-Vorgänge möglicherweise fehlschlagen, wenn SnapManager das Storage-System nicht erkennt. Sie müssen einige zusätzliche Schritte im DataFabric Manager-Server-Host und dem SnapManager-Server-Host durchführen, um dieses Problem zu lösen.

Führen Sie im DataFabric Manager-Server-Host folgende Schritte durch:

1. Löschen Sie die IP-Adresse und den Host des früheren Storage-Systems in der Host-Datei unter /etc/Hosts im DataFabric Manager Server-Host.
2. Fügen Sie die neue IP-Adresse und den neuen Host des neuen Storage-Systems in der Host-Datei unter /etc/Hosts im DataFabric Manager Server-Host hinzu.
3. Ändern Sie den Speicherhostnamen mit folgendem Befehl: dfm Host umbenennen -a old_Host_namenew_Host_Name
4. Legen Sie die neue IP-Adresse im Host fest, indem Sie den folgenden Befehl eingeben: dfm Host set old_Host_Name_or_objId hostPrimaryAddress = New_Storage_Controller_ip_address

   Sie müssen diesen Schritt nur ausführen, wenn Sie die IP-Adresse als neuen Speichersystemnamen angegeben haben.

5. Aktualisieren Sie den neuen Storage-Systemnamen im DataFabric Manager-Server-Host, indem Sie den folgenden Befehl eingeben: dfm Host diag old_Storage_Name

   Sie können überprüfen, ob der frühere Storage Controller-Name durch einen neuen Speicher-Controller-Namen ersetzt wird, indem Sie den folgenden Befehl eingeben: dfm Host discover New_Storage_Name

Führen Sie die folgenden Schritte als Root-Benutzer im SnapManager Server-Host aus.

Wenn Sie den neuen Namen des Speichercontrollers eingeben, stellen Sie sicher, dass Sie den Systemaliasnamen und nicht den vollständig qualifizierten Domänennamen (FQDN) verwenden.

1. Löschen Sie den früheren Storage-Systemnamen mit dem folgenden Befehl: SnapDrive config delete old_Storage_Name

   Wenn der frühere Name des Storage-Systems nicht gelöscht wird, schlagen alle SnapManager-Vorgänge fehl.

2. Löschen Sie die IP-Adresse und den Host des früheren Speichersystems in der Host-Datei unter etc/Hosts im Ziel-Datenbank-Host.

3. Fügen Sie die neue IP-Adresse und den neuen Host des neuen Speichersystems in der Hostdatei, die sich unter /etc/Hosts im Ziel-Datenbank-Host befindet, hinzu.
4. Geben Sie den folgenden Befehl ein, um den neuen Namen des Speichersystems hinzuzufügen: SnapDrive config set root New_Storage_Name
5. Ordnen Sie die Namen der Storage-Systeme vor und höher mit dem folgenden Befehl zu: SnapDrive config Migration set old_Storage_namenew_Storage_Name
6. Löschen Sie den Management-Pfad des früheren Storage-Systems durch Eingabe des Befehls:snapdrive config delete -mgmtpath old_Storage_Name
7. Fügen Sie den Management-Pfad für das neue Storage-System hinzu, indem Sie den folgenden Befehl eingeben: SnapDrive config set -mgmtpath New_Storage_Name
8. Aktualisieren Sie den Datensatz für Datendateien und Archivprotokolldateien mit dem neuen Speichersystemnamen durch Eingabe des folgenden Befehls: SnapDrive Dataset changehostname -dndataset_Name-oldnameold_Storage_Name-newnamenw_Storage_Name
9. Aktualisieren Sie das Profil für den neuen Namen des Speichersystems, indem Sie den folgenden Befehl eingeben: smo Storage umbenennen -profileprofile_Name-oldnameold_Storage_Name -newnamenew_Storage_Name
10. Überprüfen Sie, ob das mit dem Profil verknüpfte Storage-System durch Eingabe des folgenden Befehls: smo Storage list -profileprofile_Name

Fehlerbehebung bei bekannten Problemen

Sie sollten einige bekannte Probleme kennen, die bei der Verwendung von SnapManager auftreten können, und deren Umgang damit.

SnapManager für Oracle erkennt Cluster-Mode-Profile nicht

Falls der Clustermodus-Profilname nicht in der Datei cmode_profiles.config im Installationsverzeichnis von SnapManager für Oracle vorhanden ist, kann die folgende Fehlermeldung auslösen:

Konfigurieren Sie bitte DFM Server mit SnapDrive config set -dfm user_Name Appliance_Name.

Wenn Sie auch bei der Aktualisierung der SnapManager für Oracle den Ordner /opt/NetApp/smo/* löschen, wird auch die Datei cmode_profil.config mit den Cluster-Mode-Profilnamen gelöscht. Dieses Problem löst auch die gleiche Fehlermeldung aus.

Workaround

Aktualisieren Sie das Profil: smo Profile Update-profile <profile_Name>

> Falls SnapManager für Oracle im Pfad /opt/NetApp/smo/ installiert ist, lautet der Dateispeicherort /opt/NetApp/smo/cmode_profile.config.

Der Server kann nicht gestartet werden

Beim Starten des Servers wird möglicherweise eine Fehlermeldung wie die folgende angezeigt:

SMO-01104: Fehler beim Aufrufen des Befehls: SMO-17107: Der SnapManager Server konnte aufgrund der folgenden Fehler nicht am Port 8074 gestartet werden: java.net.BindException: die Adresse wird bereits verwendet

Dies kann daran liegen, dass die SnapManager-Listening-Ports (standardmäßig 27214 und 27215) derzeit von einer anderen Anwendung verwendet werden.

Dieser Fehler kann auch auftreten, wenn der smo_Server-Befehl bereits ausgeführt wird, aber SnapManager erkennt den vorhandenen Prozess nicht.

Workaround

Sie können SnapManager oder die andere Anwendung neu konfigurieren, um unterschiedliche Ports zu verwenden.

Um SnapManager neu zu konfigurieren, bearbeiten Sie die folgende Datei: /Opt/NTAP/smo/Properties/smo.config

Sie weisen folgende Werte zu:

- SMO Server.Port = 27214
- SMO Server.rmiRegistry.Port=27215
- Remote.Registry.ocijdbc.Port= 27215

  Der Remote.Registry.ocijdbc.Port muss der gleiche sein wie der Server.rmiRegistry.Port.

Geben Sie zum Starten des SnapManager-Servers den folgenden Befehl ein: smo_Server starte

Wenn der Server bereits ausgeführt wird, wird eine Fehlermeldung angezeigt.

Wenn der Server bereits ausgeführt wird, führen Sie die folgenden Schritte aus:

1. Beenden Sie den Server, indem Sie den folgenden Befehl eingeben: smo_Server stop
2. Starten Sie den Server neu, indem Sie den folgenden Befehl eingeben: smo_Server Start

Beenden eines derzeit ausgeführten SnapManager-Vorgangs

Wenn der SnapManager-Server ausfällt und Sie keine Vorgänge erfolgreich ausführen können, können Sie SnapManager und seine Vorgänge beenden.

Workaround

SnapManager arbeitet mit SnapManager und Protection Manager zusammen. Sie müssen die folgenden Schritte durchführen, um die verschiedenen laufenden Prozesse aufzuführen und den zuletzt ausgeführten Prozess zu beenden.

1. Listen Sie alle laufenden SnapDrive Prozesse auf: ps

   Beispiel: ps/grep SnapDrive

2. Beenden Sie den SnapDrive-Prozess oder die Prozesse: Kill <PID>

   pid ist die Liste der Prozesse, die Sie mit dem Befehl ps gefunden haben.

   Stoppen Sie nicht alle SnapDrive Prozesse. Möglicherweise möchten Sie nur den letzten laufenden Prozess beenden.

3. Wenn einer der Vorgänge die Wiederherstellung eines geschützten Backups aus dem sekundären Storage beinhaltet, öffnen Sie die Protection Manager Konsole und führen Sie Folgendes aus:
   a. Wählen Sie im Menü System die Option **Jobs** aus.
   b. Wählen Sie **Wiederherstellen**.
   c. Überprüfen Sie, ob der Name des Datensatzes mit dem im SnapManager-Profil übereinstimmt.
   d. Klicken Sie mit der rechten Maustaste, und wählen Sie **Abbrechen**.
4. Auflisten der SnapManager-Prozesse:
   a. Melden Sie sich als Root-Benutzer an.
   b. Führen Sie die Prozesse mit dem Befehl ps auf.

      Beispiel: ps/grep java
5. Beenden Sie den SnapManager-Prozess: Kill <PID>

Das letzte geschützte Backup kann nicht gelöscht oder gelöscht werden

Wenn Sie das erste Backup für ein Profil auf dem sekundären Storage erstellen, sendet SnapManager alle Informationen zum Backup an den Protection Manager. Bei nachfolgenden Backups zu diesem Profil sendet SnapManager nur die geänderten Informationen. Wenn Sie das letzte geschützte Backup entfernen, verliert SnapManager die Möglichkeit, die Unterschiede zwischen Backups zu identifizieren und muss eine Möglichkeit finden, diese Beziehungen neu zu erstellen. Daher wird beim Löschen des letzten geschützten Backups eine Fehlermeldung angezeigt.

Workaround

Sie können das Profil oder nur das Profil-Backup löschen.

So löschen Sie das Profil:

1. Löschen Sie die Backups des Profils.
2. Aktualisieren Sie das Profil, und deaktivieren Sie den Schutz im Profil.

   Dadurch wird der Datensatz gelöscht.
3. Löschen Sie das letzte geschützte Backup.
4. Löschen Sie das Profil.

Führen Sie die folgenden Schritte aus, um nur das Backup zu löschen:

1. Erstellen Sie eine weitere Sicherungskopie des Profils.
2. Übertragen der Backup-Kopie auf den sekundären Storage.
3. Löschen Sie die vorherige Backup-Kopie.

Zielnamen der Archivprotokolldatei können nicht verwaltet werden, wenn die Zielnamen Teil anderer Zielnamen sind

Wenn der Benutzer beim Erstellen einer Archiv-Log-Sicherung ein Ziel ausschließt, das Teil anderer Zielnamen ist, werden auch die anderen Zielnamen ausgeschlossen.

Angenommen, es gibt drei Ziele, die ausgeschlossen werden können: /Dest, /dest1 und /dest2. Beim Erstellen

der Backup der Archivprotokolldatei, wenn Sie /dest mit dem Befehl ausschließen

```
smo backup create -profile almsamp1 -data -online -archivelogs  -exclude
-dest /dest
```

, SnapManager für Oracle schließt alle Ziele ab, die mit /dest beginnen.

Workaround

- Fügen Sie einen Pfadtrenner hinzu, nachdem Ziele in V€tarchiv_dest konfiguriert wurden. Ändern Sie z. B. /dest in /dest/.
- Bei der Erstellung eines Backups sollten Ziele berücksichtigt werden, anstatt Ziele auszuschließen.

Die Wiederherstellung von Steuerdateien, die auf Automatic Storage Management (ASM) und nicht-ASM-Speicher multipliziert werden, schlägt fehl

Wenn die Steuerdateien auf ASM- und nicht-ASM-Speicher multipliziert werden, ist der Backup-Vorgang erfolgreich. Wenn Sie jedoch versuchen, Steuerdateien aus diesem erfolgreichen Backup wiederherzustellen, schlägt der Wiederherstellungsvorgang fehl.

Der SnapManager Klonvorgang ist fehlgeschlagen

Wenn Sie ein Backup in SnapManager klonen, kann der DataFabric Manager Server Volumes möglicherweise nicht erkennen und die folgende Fehlermeldung anzeigen:

SMO-13032: Vorgang kann nicht ausgeführt werden: Clone Create. Root Cause: SMO-11007: Fehler beim Klonen vom Snapshot: FLOW-11019: Ausfall in ExecuteConnectionSteps: SD-00018: Fehler beim Erkennen von Storage für /mnt/datafile_clone3: SD-10016: Fehler beim Ausführen des SnapDrive Befehls "/usr/sbin/snapdrive Storage show -fs /mnt/datafile_clone3“: 0002-719 Warnung: Konnte nicht überprüft werden.SD Storage.Lesezugriff auf dem Volume: Manager:/vol_\Server:.1_vol_Manager auf dem benutzer.x1_20091122235002515

Grund: Ungültige Ressource angegeben. Seine ID wurde auf dem Operations Manager-Server 10.x.x.x nicht gefunden

Dies geschieht, wenn das Storage-System über eine große Anzahl von Volumes verfügt.

Workaround

Sie müssen einen der folgenden Schritte ausführen:

- Führen Sie auf dem Data Fabric Manager-Server dfm Host discover Storage_System aus.

  Sie können den Befehl auch in eine Shell-Skript-Datei hinzufügen und einen Job im DataFabric Manager-Server planen, um das Skript in einem regelmäßigen Intervall zu ausführen.

- Erhöhen Sie den Wert von dfm-rbac-Wiederholungen in der SnapDrive.conf Datei.

  SnapDrive verwendet den Standardwert für das Aktualisierungsintervall und die Standardanzahl von Wiederholungen. der Standardwert von dfm-rbac-retry-Sleep-Sek. ist 15 Sekunden und dfm-rbac-Wiederholungen ist 12 Iterationen.

Das Operations Manager-Aktualisierungsintervall hängt von der Anzahl der Storage-Systeme, der Anzahl der Storage-Objekte im Storage-System und der Last auf dem DataFabric Manager-Server ab.

Führen Sie als Empfehlung Folgendes aus:

a. Führen Sie auf dem DataFabric Manager-Server den folgenden Befehl manuell für alle sekundären Speichersysteme aus, die mit dem Datensatz verbunden sind: dfm Host discover Storage_System
b. Verdoppeln Sie die für die Host-Erkennung benötigte Zeit und weisen sie diesen Wert DFM-rbac-retry-Sleep-Sek. zu.

   Wenn der Vorgang beispielsweise 11 Sekunden in Anspruch nahm, können Sie den Wert von dfm-rbac-retry-Sleep-Sek. auf 22 (11*2) setzen.

Die Größe der Repository-Datenbank wächst mit der Zeit, nicht mit der Anzahl der Backups

Die Größe der Repository-Datenbank wächst mit der Zeit, da SnapManager-Operationen Daten innerhalb des Schemas in den Repository-Datenbanktabellen einfügen oder löschen, was zu einer hohen Indexbelegung führt.

Workaround

Sie müssen die Indizes gemäß den Oracle-Richtlinien überwachen und neu erstellen, um den vom Repository-Schema belegten Speicherplatz zu steuern.

Auf die SnapManager-Benutzeroberfläche kann nicht zugegriffen werden und SnapManager-Vorgänge schlagen fehl, wenn die Repository-Datenbank ausfällt

SnapManager-Vorgänge schlagen fehl und Sie können nicht auf die GUI zugreifen, wenn die Repository-Datenbank ausfällt.

In der folgenden Tabelle sind die verschiedenen Aktionen aufgeführt, die Sie ausführen möchten, sowie deren Ausnahmen:

Betrieb	Ausnahmen
Öffnen eines geschlossenen Repository	Die folgende Fehlermeldung wird in SM_gui.log: [WARNUNG]: SMO-01106: Beim Abfragen des Projektarchivs ist ein Fehler aufgetreten: Geschlossene Verbindung java.sql.SQLException: Geschlossene Verbindung.
Aktualisieren eines geöffneten Projektarchivs durch Drücken von F5	Eine Projektarchiv-Ausnahme wird in der GUI angezeigt und protokolliert auch eine NullPointerException in der Datei sm_gui.log.
Aktualisieren des Hostservers	Eine NullPointerException wird in der Datei sumo_gui.log protokolliert.
Erstellen eines neuen Profils	Im Fenster Profilkonfiguration wird eine NullPointerException angezeigt.

Aktualisieren eines Profils	Die folgende SQL-Ausnahme wird in SM_gui.log: [WARNUNG] protokolliert: SMO-01106: Beim Abfragen des Projektarchivs ist ein Fehler aufgetreten: Geschlossene Verbindung.
Zugriff auf ein Backup	Die folgende Fehlermeldung wird in SM_gui.log protokolliert: Die Initialisierung einer Sammlung konnte nicht abgeschlossen werden.
Anzeigen der Kloneigenschaften	Die folgende Fehlermeldung wird in sm_gui.log protokolliert und sumo_gui.log: Die Initialisierung einer Sammlung konnte nicht abgeschlossen werden.

Workaround

Sie müssen sicherstellen, dass die Repository-Datenbank ausgeführt wird, wenn Sie auf die GUI zugreifen möchten oder SnapManager-Vorgänge ausführen möchten.

Es können keine temporären Dateien für die geklonte Datenbank erstellt werden

Wenn temporäre Tablespaces-Dateien der Zieldatenbank in Mount-Punkten platziert werden, die sich vom Mount-Punkt der Datendateien unterscheiden, ist der Klonvorgang erfolgreich, SnapManager kann jedoch keine temporären Dateien für die geklonte Datenbank erstellen.

Workaround

Sie müssen einen der folgenden Schritte ausführen:

- Stellen Sie sicher, dass die Zieldatenbank so angelegt ist, dass temporäre Dateien an demselben Bereitstellungspunkt wie die der Datendateien abgelegt werden.
- Manuelles Erstellen oder Hinzufügen temporärer Dateien in der geklonten Datenbank.

Die Migration des Protokolls von NFSv3 zu NFSv4 ist nicht möglich

Sie können das Protokoll von NFSv3 zu NFSv4 migrieren, indem Sie den Parameter enable-migrate-nfs-Version in der Datei snapdrive.conf aktivieren. Während der Migration betrachtet SnapDrive nur die Protokollversion, unabhängig von den Mount-Point-Optionen wie rw, Forellenfiles, Nosuid usw.

Wenn Sie jedoch nach der Migration des Protokolls auf NFSv4 den Backup wiederherstellen, der mit NFSv3 erstellt wurde, tritt Folgendes auf:

- Wenn NFSv3 und NFSv4 auf Storage-Ebene aktiviert sind, ist die Wiederherstellung erfolgreich, wird aber mit den Mount-Point-Optionen bereitgestellt, die während des Backups verfügbar waren.
- Wenn nur NFSv4 auf Storage-Ebene aktiviert ist, ist der Wiederherstellungsvorgang erfolgreich und nur die Protokollversion (NFSv4) bleibt erhalten.

  Die anderen Mount-Punkt-Optionen wie rw, Forellenfiles, Nosuid usw. werden jedoch nicht beibehalten.

Workaround

Sie müssen die Datenbank manuell herunterfahren, die Mount-Punkte der Datenbank aufheben und mit den

vor der Wiederherstellung verfügbaren Optionen mounten.

Das Backup der Data Guard Standby-Datenbank ist fehlgeschlagen

Wenn ein Archivprotokoll mit dem Dienstnamen der primären Datenbank konfiguriert ist, schlägt die Datensicherung der Data Guard Standby-Datenbank fehl.

Workaround

In der GUI müssen Sie **External Archive Log Location** angeben, der dem Dienstnamen der primären Datenbank entspricht.

Montage eines FlexClone Volume schlägt in der NFS-Umgebung fehl

Wenn SnapManager einen FlexClone eines Volumes in einer NFS-Umgebung erstellt, wird in der Datei /etc/exports ein Eintrag hinzugefügt. Der Klon oder das Backup kann nicht auf einem SnapManager Host mit einer Fehlermeldung gemountet werden.

Die Fehlermeldung ist: 0001-034 Befehlsfehler: Mount fehlgeschlagen: Mount: Filer1:/vol/SnapManager_20090914112850837_vol14 auf /opt/NTAPsmo/mnt/-ora_data02-20090914112850735_1 - WARNUNG unbekannte Option „Zone=vol14“ nfs Mount: Filer1:/vol/SnapManager_20090914112850837_vol14: Berechtigung verweigert.

Gleichzeitig wird an der Storage System Console folgende Meldung erzeugt: Mon Sep 14 23:58:37 PDT [filer1: export.auto.update.disabled: Warnung]: /Etc/exports wurde für vol14 nicht aktualisiert, wenn der Befehl vol Clone create ausgeführt wurde. Aktualisieren Sie /etc/exports manuell oder kopieren Sie /etc/exports.New.

Diese Meldung wird möglicherweise nicht in den AutoSupport-Meldungen erfasst.

Sie können ähnliche Probleme beim Klonen von FlexVol Volumes auf NFS auftreten. Sie können die gleichen Schritte ausführen, um die Option nfs.export.auto-update zu aktivieren.

Was zu tun

1. Stellen Sie die Option nfs.export.auto-update ein, damit die Datei /etc/exports automatisch aktualisiert wird. Optionen nfs.export.auto-updateon

Stellen Sie in der Konfiguration des HA-Paars sicher, dass Sie die NFS-Exportoption für beide Storage-Systeme auf ON setzen.

Ausführung mehrerer paralleler Vorgänge schlägt in SnapManager fehl

Wenn Sie mehrere parallele Vorgänge auf separaten Datenbanken ausführen, die sich im selben Storage-System befinden, wird die Initiatorgruppe für LUNs, die beiden Datenbanken zugeordnet sind, möglicherweise aufgrund eines der Vorgänge gelöscht. Wenn später der andere Vorgang versucht, die gelöschte Initiatorgruppe zu verwenden, zeigt SnapManager eine Fehlermeldung an.

Wenn beispielsweise Backup-Löschvorgänge und Backup-Erstellungsvorgänge für verschiedene Datenbanken nahezu gleichzeitig ausgeführt werden, schlägt der Backup-Vorgang fehl. Die folgenden sequenziellen Schritte zeigen, was passiert, wenn Sie Backup löschen und Backup erstellen Vorgänge auf verschiedenen Datenbanken fast gleichzeitig ausführen.

1. Führen Sie den Befehl Backup delete aus.
2. Führen Sie den Befehl Backup create aus.
3. Der Befehl zum Erstellen des Backups identifiziert die bereits vorhandene Initiatorgruppe und verwendet dieselbe Initiatorgruppe zum Zuordnen der LUN.
4. Der Befehl zum Löschen des Backups löscht die Backup-LUN, die derselben Initiatorgruppe zugeordnet war.
5. Mit dem Befehl „Backup löschen“ wird dann die Initiatorgruppe gelöscht, da der Initiatorgruppe keine LUNs zugeordnet sind.
6. Der Befehl „Backup create“ erstellt das Backup und versucht, der Initiatorgruppe, die nicht vorhanden ist, zuzuordnen. Somit schlägt der Vorgang fehl.

Was zu tun

Sie müssen eine Initiatorgruppe für jedes von der Datenbank verwendete Storage-System erstellen und SDU mit dem folgenden Befehl mit den igroup-Informationen aktualisieren: SnapDrive igroup hinzufügen

RAC-Datenbank kann von einem der RAC-Knoten, in dem das Profil nicht erstellt wurde, nicht wiederhergestellt werden

In einer Oracle RAC Umgebung, in der beide Nodes zum selben Cluster gehören, wenn Sie einen Wiederherstellungsvorgang von einem Node starten, der sich von dem Node, an dem das Backup erstellt wurde, unterscheidet, schlägt der Wiederherstellungsvorgang fehl.

Wenn Sie beispielsweise in Knoten A ein Backup erstellen und versuchen, von Knoten B wiederherzustellen, schlägt der Wiederherstellungsvorgang fehl.

Was zu tun

Führen Sie vor dem Durchführen des Wiederherstellungsvorgangs von Node B folgende Schritte in Node B durch:

1. Fügen Sie das Repository hinzu.
2. Synchronisieren Sie das Profil, indem Sie das Kommando smo profile Sync ausführen.
3. Legen Sie die Anmeldeinformationen für das Profil fest, das für den Wiederherstellungsvorgang verwendet werden soll, indem Sie den Befehlssatz für Smo-Anmeldeinformationen ausführen.
4. Aktualisieren Sie das Profil, um den neuen Hostnamen und den entsprechenden SID hinzuzufügen, indem Sie den Befehl smo Profil aktualisieren.

Weitere Informationen

Hier finden Sie Informationen zu den grundlegenden Aufgaben, die bei der Installation und Verwendung von SnapManager anfallen.

Dokument An	Beschreibung
Beschreibungsseite „SnapManager“	Auf dieser Seite finden Sie Informationen über SnapManager, Verweise auf Online-Dokumentationen und einen Link zur SnapManager Download-Seite, von der aus Sie die Software herunterladen können.
Data ONTAP-SAN-Konfigurationsleitfaden für 7-Mode	Dieses Dokument ist unter verfügbar "mysupport.netapp.com". Es handelt sich um ein dynamisches Online-Dokument mit aktuellsten Informationen zu den Anforderungen für das Einrichten eines Systems in einer SAN-Umgebung. Er liefert die aktuellen Details zu Storage-Systemen und Host-Plattformen, Verkabelungsproblemen, Switch-Problemen und Konfigurationen.
Kompatibilitätsmatrix für SnapManager und SnapDrive	Dieses Dokument ist im Abschnitt Interoperabilität verfügbar unter "mysupport.netapp.com/matrix". Es handelt sich um ein dynamisches Online-Dokument, das die aktuellsten Informationen enthält, die für SnapManager und seine Plattformanforderungen spezifisch sind.
Versionshinweise zu SnapManager	Dieses Dokument ist mit SnapManager erhältlich. Sie können auch eine Kopie von herunterladen "mysupport.netapp.com". Es enthält alle Last-Minute-Informationen, damit die Konfiguration reibungslos ausgeführt werden kann.
Dokumentation von NetApp Host-Anschluss und Support-Kits	"mysupport.netapp.com".
Systemkonfigurationshandbuch	"mysupport.netapp.com".
Data ONTAP Block Access Management-Leitfaden	"mysupport.netapp.com"
Informationen zu Host-Betriebssystem und Datenbank	Diese Dokumente enthalten Informationen zu Ihrem Host-Betriebssystem und Ihrer Datenbanksoftware.

Klassifizierungen für Fehlermeldungen

Sie können die Ursache eines Fehlers bestimmen, wenn Sie die Klassifizierungen der Nachrichten kennen.

In der folgenden Tabelle finden Sie Informationen zu den numerischen Bereichen für die verschiedenen Meldungsarten, die Sie möglicherweise bei SnapManager sehen:

Gruppieren	Bereich	Zu Verwenden
UMGEBUNG	1000-1999	Wird verwendet, um den Zustand oder Probleme mit der Betriebsumgebung von SnapManager zu protokollieren. Diese Gruppe umfasst Meldungen über die Systeme, mit denen SnapManager interagiert, wie z. B. Host, Storage-System, Datenbank usw.
BACKUP	2000-2999	Verbunden mit dem Datenbank-Backup-Prozess.
WIEDERHERSTELLEN	3000-3999	Verknüpft mit dem Wiederherstellungsprozess der Datenbank.
KLON	4000-4999	Diesem Datenbankklonprozess zugeordnet.
PROFIL	5000-5999	Wird zum Verwalten von Profilen verwendet.
MANAGEN	6000-6999	Wird für das Management von Backups verwendet.
SCHNITTSTELLE FÜR VIRTUELLE DATENBANKEN	7000-7999	Der Schnittstelle der virtuellen Datenbank zugeordnet.
VIRTUAL STORAGE INTERFACE	8000-8999	Einer virtuellen Storage-Schnittstelle zugeordnet.
REPOSITORY	9000-9999	Der Repository-Schnittstelle zugeordnet.
METRIKEN	10000-10999	Zugeordnet zur Größe des Datenbank-Backups, verstrichene Zeit zum Backup, Zeit zur Wiederherstellung der Datenbank, die Anzahl der Male, die eine Datenbank geklont wurde usw.
VIRTUELLE HOST-SCHNITTSTELLE	11000-11999	Der virtuellen Host-Schnittstelle zugeordnet. Dies ist die Schnittstelle zum Host-Betriebssystem.

Gruppieren	Bereich	Zu Verwenden
AUSFÜHRUNG	12000-12999	Verbunden mit dem Ausführungspaket, einschließlich Laichen und Verarbeitung von Betriebssystemaufrufen.
PROZESS	13000-13999	Verknüpft mit der Prozesskomponente von SnapManager.
VERSORGUNGSUNTERNEHMEN	14000-14999	Verbunden mit SnapManager Utilities, globalem Kontext usw.
DUMP/DIAGNOSE	15000-15999	Im Zusammenhang mit Dump- oder Diagnosevorgängen.
HILFE	16000-16999	Mit Hilfe verknüpft.
SERVER	17000-17999	Wird in der SnapManager-Serveradministration verwendet.
API	18000-18999	Der API zugeordnet.
AUTH	20000-20999	Mit der Autorisierung von Anmeldeinformationen verknüpft.

Fehlermeldungen

Sie finden Informationen zu den Fehlermeldungen, die mit verschiedenen SnapManager Vorgängen verbunden sind.

Die häufigsten Fehlermeldungen

Die folgende Tabelle enthält einige der häufigsten und wichtigsten Fehler im Zusammenhang mit SnapManager für Oracle:

Fehlermeldung	Erklärung	Auflösung
SD-10038: Dateisystem ist nicht beschreibbar.	Der SnapManager-Prozess hat keinen Schreibzugriff auf das Dateisystem.	Sie müssen sicherstellen, dass der SnapManager-Prozess Schreibzugriff auf das Dateisystem hat. Nach der Korrektur müssen Sie eventuell einen weiteren Snapshot erstellen.

Fehlermeldung	Erklärung	Auflösung
SMO-05075: Profil konnte nicht erstellt werden. Sie müssen die DP/XDP-Beziehung entsprechend der zugrunde liegenden Beziehung richtig konfigurieren oder die richtige Schutzrichtlinie auswählen.	Die zugrunde liegenden Volumes befinden sich nicht in einer SnapVault oder SnapMirror Beziehung.	Sie müssen eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.
SMO-05503: Sie haben denselben Namen für das Profil angegeben. Geben Sie einen anderen Namen an, um das Profil umzubenennen.	Profile mit identischen Namen können nicht in einem Repository vorhanden sein.	Geben Sie einen Profilnamen an, der nicht verwendet wird.
SMO-05505: Die Metadaten des Datensatzes können nicht aktualisiert werden.	Datensatz wurde möglicherweise gelöscht oder ist nicht vorhanden.	Vergewissern Sie sich vor dem Aktualisieren der Datensatz-Metadaten, dass der Datensatz mithilfe der NetApp Management Console vorhanden ist.
SMO-05506: Sie können das Profil nicht aktualisieren, da auf dem Profil Operationen ausgeführt werden. Sie müssen warten, bis die Operation(en) abgeschlossen ist und dann das Profil aktualisieren.	Profil kann nicht aktualisiert werden, wenn Backup-, Wiederherstellungs- und Klonvorgänge ausgeführt werden.	Aktualisieren Sie das Profil nach Abschluss des aktuellen Vorgangs.
SMO-05509: Ungültige primäre Aufbewahrungsdauer beim Archivprotokoll - geben Sie einen positiven Ganzzahl an.	Die Aufbewahrungsdauer von Backups im Archivprotokoll kann nicht negativ sein.	Geben Sie einen positiven Wert für die Aufbewahrungsdauer von Archiv-Log-Backups an.
SMO-07463: Für diese Backup-Wiederherstellung muss die Datenbank im erforderlichen Zustand sein. Fehler beim Abrufen der Datenbank in den erforderlichen Zustand.	Die Datenbank befindet sich nicht im erforderlichen Zustand für einen Backup-Vorgang.	Überprüfen Sie, ob die Datenbank in einem relevanten Zustand ist, bevor Sie eine Backup-Kopie erstellen. Der Status der Datenbank, die wiederhergestellt werden soll, hängt von der Art des Wiederherstellungsprozesses, die Sie durchführen möchten, und der Art der Dateien ab, die enthalten sein sollen.

Fehlermeldung	Erklärung	Auflösung
SMO-09315: Nach Durchführung von Repository-Upgrades oder -Updates erhalten Sie möglicherweise keine zusammenfassende Benachrichtigung für Benachrichtigungen, die in der vorherigen Version festgelegt wurden, es sei denn, Sie aktualisieren die Zusammenfassung Benachrichtigung mit den Details des Benachrichtigungs-Hosts.	Benachrichtigungseinstellungen sind nach einem Rolling Upgrade nicht für das Repository konfiguriert.	Aktualisieren Sie nach einem Rolling Upgrade die Benachrichtigungseinstellungen für die Zusammenfassung, um Benachrichtigungen zu erhalten.
SM0-02076: Der Name des Etiketts darf keine Sonderzeichen enthalten, die nicht unterstrich sind.	Der Name des Etiketts enthält Sonderzeichen, die nicht vom Unterstrich verwendet werden.	Der Name der Bezeichnung muss innerhalb des Profils eindeutig sein. Der Name kann Buchstaben, Zahlen, einen Unterstrich (_) und einen Bindestrich (-) enthalten (kann jedoch nicht mit einem Bindestrich beginnen). Achten Sie darauf, dass Etiketten keine Sonderzeichen enthalten, außer dem Unterstrich.
SMO-06308: Ausnahme beim Versuch, Zeitplan zu starten: java.lang.NullPointerException	Der vollständig qualifizierte Domänenname (FQDN) des Profilhosts ist anstelle des Host-Namens des Systems konfiguriert, und der FQDN des Profilhosts kann nicht aufgelöst werden.	Stellen Sie sicher, dass Sie den Hostnamen des Systems und nicht den FQDN verwenden.
Fehler in ExecuteRestoreSteps: ORACLE-10003: Fehler beim Ausführen von SQL "DROP DISKGROUP;Control diskgroup Name; INCL. INHALT" gegen Oracle-Datenbank +ASM1: ORA-15039: diskgroup not Drop ORA-15027: Aktive Nutzung der Diskgroup; "Control diskgroup Name;" schließt seine Dismount aus	Der Vorgang zum Wiederherstellen eines Backups mit Steuerdateien fällt nicht auf die Steuerplattengruppe. Dieses Problem tritt auf, wenn veraltete gesicherte Kontrolldateien in der Gruppe der Steuerdatenträger vorhanden sind.	Identifizieren Sie die veralteten gesicherten Kontrolldateien, und löschen Sie sie manuell.

Fehlermeldung	Erklärung	Auflösung
RMAN-06004: ORACLE-Fehler aus der Datenbank des Wiederherstellungskatalogs: ORA-01424: Fehlende oder unzulässige Zeichen nach dem Escape-Zeichen	Beim Erstellen des Backups konnte die Backup-Kopie nicht aus dem Katalog entfernt werden, wenn SnapManager in RMAN integriert ist.	Überprüfen Sie, ob externe Skripts zum Entfernen der Backups aus RMAN verwendet werden. Führen Sie DEN CROSSCHECK-BACKUP-Befehl in RMAN aus, um das RMAN-Repository zu aktualisieren und den Befehl „Resynchronisieren“-Katalog, um die Steuerdatei der Zieldatenbank mit dem Wiederherstellungskatalog zu synchronisieren.
[DEBUG]: Ausnahme beim Beschneiden von Backups. java.lang.IllegalStelleException: [Assertion failed] - dieser Zustand invariant muss wahr sein	Mehrere Snapshot Kopien werden für eine einzige Operation ID erstellt.	Löschen Sie die Snapshot-Kopien manuell, und löschen Sie die Einträge mithilfe von Skripten aus dem Repository.
Die Systemzeit und die von SnapManager in den Protokolldateien angezeigte Zeit stimmen nicht überein oder nicht synchronisiert.	Eine Änderung der Zeitzone wird von Java 7 noch nicht unterstützt.	Wenden Sie den von Oracle bereitgestellten tzupdater-Patch an.
DISC-00001: Speicher kann nicht gefunden werden: Die folgende Kennung existiert nicht oder ist nicht vom erwarteten Typ: ASM-Datei	Daten- oder Kontrolldateien oder Redo-Logs werden in einer ASM-Datenbank multipliziert.	Entfernen Sie das Oracle Multiplexing.
ORA-01031: Unzureichende Berechtigungen. Überprüfen Sie, ob der SnapManager-Windows-Dienst so eingerichtet ist, dass er als Benutzer mit den richtigen Berechtigungen ausgeführt wird und dass der Benutzer in die ORA_DBA-Gruppe aufgenommen wurde.	In SnapManager verfügen Sie über unzureichende Berechtigungen. Das SnapManager-Dienstkonto ist nicht Teil der ORA_DBA-Gruppe.	Klicken Sie mit der rechten Maustaste auf das Symbol **Computer** auf Ihrem Desktop und wählen Sie **Verwalten** aus, um zu überprüfen, ob das Benutzerkonto für den SnapManager-Dienst Teil der ORA_DBA-Gruppe ist. Überprüfen Sie lokale Benutzer und Gruppen und stellen Sie sicher, dass das Konto Teil der ORA_DBA-Gruppe ist. Wenn der Benutzer der lokale Administrator ist, stellen Sie sicher, dass sich der Benutzer in der Gruppe und nicht in der Domain-Administrator befindet.

Fehlermeldung	Erklärung	Auflösung
0001-CON-10002: Verbundene ASM-Laufwerke mit Pfaden <paths> wurden von der ASM-Instanz <asm_Instance_sid> nicht erkannt. Überprüfen Sie, ob die Parameter ASM_DISKSTRING und die Dateisystemberechtigungen diese Pfade ermöglichen.	ASM-Laufwerke waren mit dem Host verbunden, aber die ASM-Instanz ist nicht in der Lage, sie zu erkennen.	Wenn ASM über NFS verwendet wird, stellen Sie sicher, dass der Parameter ASM_DISKSTRING für die ASM-Instanz die ASM-Festplattendateien enthält. Wenn der Fehler z. B. Folgendes angibt: smo/mnt/<dir_Name>/<Disk_Name>, fügen Sie /smo/mnt// zu asm_diskstring hinzu.
0001-DS-10021: Sicherungsrichtlinie des Datensatzes <Dataset-Name> kann nicht auf <New-Protection-Policy> festgelegt werden, da die Sicherungsrichtlinie bereits auf <old-Protection-Policy> festgelegt ist. Bitte verwenden Sie Protection Manager, um die Schutzrichtlinie zu ändern	Nachdem die Sicherungsrichtlinie eines Datensatzes festgelegt wurde, können Sie mit SnapManager die Sicherungsrichtlinie nicht ändern, da unter Umständen die Basisbeziehungen neu ausgerichtet werden müssen und es zu dem Verlust vorhandener Backups auf dem Sekundärspeicher kommen muss.	Aktualisieren Sie die Sicherungsrichtlinie mithilfe der Management Console von Protection Manager, die mehr Optionen zur Migration von einer Schutzrichtlinie zu einer anderen bietet.
0001-SD-10028: SnapDrive-Fehler (id:2618 Code:102) das mit "lun_PATH" verknüpfte Gerät konnte nicht gefunden werden. Wenn Multipathing in Verwendung ist, kann ein möglicher Multipathing-Konfigurationsfehler verwendet werden. Bitte Konfiguration überprüfen und wiederholen.	Der Host kann keine LUNs erkennen, die auf den Speichersystemen erstellt wurden.	Stellen Sie sicher, dass das Transportprotokoll ordnungsgemäß installiert und konfiguriert ist. Stellen Sie sicher, dass SnapDrive eine LUN auf dem Speichersystem erstellen und erkennen kann.
0001-SD-10028: SnapDrive-Fehler (id:2836 Code:110) Datensatz-Sperre auf Datenträger "Speichername":"temp_Volume_Name" konnte nicht erfasst werden	Sie haben versucht, die Wiederherstellung mit der Methode für den indirekten Speicher durchzuführen, und das angegebene temporäre Volume ist nicht im primären Speicher vorhanden.	Erstellen eines temporären Volumes auf dem primären Storage Oder geben Sie den korrekten Volume-Namen an, falls bereits ein temporäres Volume erstellt wurde.

Fehlermeldung	Erklärung	Auflösung
0001-SMO-02016: Es können externe Tabellen in der Datenbank vorhanden sein, die nicht im Rahmen dieses Backup gesichert wurden (da die Datenbank während dieses Backups nicht GEÖFFNET war, konnten ALL_EXTERNAL_LOCATIONS nicht abgefragt werden, um festzustellen, ob externe Tabellen vorhanden sind oder nicht).	Externe Tabellen werden von SnapManager nicht gesichert (z. B. Tabellen, die nicht in .dbf-Dateien gespeichert sind). Dieses Problem tritt auf, weil die Datenbank während des Backups nicht geöffnet war. SnapManager kann nicht bestimmen, ob externe Tabellen verwendet werden.	Möglicherweise gab es externe Tabellen in der Datenbank, die im Rahmen dieses Vorgangs nicht gesichert wurden (da die Datenbank während des Backups nicht geöffnet war).
0001-SMO-11027: Snapshots können nicht vom sekundären Storage geklont oder gemountet werden, da die Snapshots beschäftigt sind. Versuchen Sie, aus einem älteren Backup zu klonen oder anzuhängen.	Sie haben versucht, einen Klon zu erstellen oder Snapshot-Kopien aus dem sekundären Storage des neuesten geschützten Backups einzubinden.	Klonen oder Mounten aus einem älteren Backup
0001-SMO-12346: Sicherungsrichtlinien können nicht aufgeführt werden, da Protection Manager Produkt nicht installiert ist oder SnapDrive nicht für die Verwendung konfiguriert ist. Installieren Sie den Protection Manager und/oder konfigurieren Sie SnapDrive…	Sie haben versucht, Schutzrichtlinien für ein System aufzulisten, das SnapDrive nicht für die Verwendung von Protection Manager konfiguriert ist.	Installieren Sie Protection Manager und konfigurieren Sie SnapDrive so, dass der Protection Manager verwendet wird.
0001-SMO-13032: Vorgang kann nicht ausgeführt werden: Backup Löschen. Ursache: 0001-SMO-02039: Backup des Datensatzes kann nicht gelöscht werden: SD-10028: SnapDrive Fehler (id:2406 Code:102) Backup-id konnte nicht gelöscht werden: „Backup_id“ für Datensatz, Fehler(23410):Snapshot „Snapshot_Name“ auf dem Volumen „Volume_Name“ ist beschäftigt.	Sie haben versucht, das neueste geschützte Backup oder ein Backup mit Snapshot-Kopien freizumachen oder zu löschen, die die Baselines in einer Mirror-Beziehung sind.	Löschen oder löschen Sie das geschützte Backup.

Fehlermeldung	Erklärung	Auflösung
0002-332 Admin-Fehler: SD.Snapshot.Clone-Zugriff auf Volume „Volume_Name“ für Benutzer-Benutzername auf Operations Manager Server(s) „dfm_Server“ konnte nicht überprüft werden. Grund: Ungültige Ressource angegeben. Kann seine ID auf Operations Manager Server „dfm_Server“ nicht finden	Die richtigen Zugriffsberechtigungen und Rollen sind nicht festgelegt.	Legen Sie Zugriffsberechtigungen oder -Rollen für die Benutzer fest, die versuchen, den Befehl auszuführen.
[WARNUNG] FLOW-11011: Vorgang abgebrochen [FEHLER] FLOW-11008: Vorgang fehlgeschlagen: Java-Heap-Speicherplatz.	Die Datenbank enthält mehr Archivprotokolldateien als die maximal zulässige Anzahl.	1. Navigieren Sie zum Installationsverzeichnis für SnapManager. 2. Öffnen Sie die Datei Launch-java. 3. Erhöhen Sie den Wert des `java -Xmx160m` Java Heap Space Parameter . So können Sie beispielsweise den Wert vom Standardwert von 160m bis 200m AS ändern `java -Xmx200m`.
SD-10028: SnapDrive Fehler (id:2868 Code:102) der Remote-Snapshot oder Remote-qtree konnte nicht gefunden werden.	SnapManager zeigt die Backups auch dann als geschützt an, wenn der Sicherungsauftrag im Protection Manager nur zum Teil erfolgreich ist. Diese Bedingung tritt auf, wenn die Datensatzkonformität erreicht wird (wenn die Basis-Snapshots gespiegelt werden).	Führen Sie ein neues Backup durch, nachdem der Datensatz inaktiv ist.
SMO-21019: Fehler beim Beschneiden des Archivprotokolls für das Ziel: "/mnt/Destination_Name/" mit dem Grund: "ORACLE-00101: Fehler beim Ausführen des RMAN-Befehls: [NOPROMPT ARCHIVELOG '/mnt/Destination_Name/' LÖSCHEN]	Die Beschneidung des Archivprotokolls schlägt in einem der Ziele fehl. In einem solchen Szenario, SnapManager weiterhin die Archiv-Log-Dateien aus den anderen Zielen zu beschneiden. Wenn Dateien manuell aus dem aktiven Dateisystem gelöscht werden, kann RMAN die Archivprotokolldateien nicht von diesem Ziel beschneiden.	Verbinden Sie sich über den SnapManager-Host mit RMAN. Führen Sie den Befehl RMAN CROSSCHECK ARCHIVELOG ALL aus und führen Sie den Beschneiungsvorgang für die Archivprotokolldateien erneut durch.

Fehlermeldung	Erklärung	Auflösung
SMO-13032: Vorgang kann nicht ausgeführt werden: Archiv-Log Prune. Root Cause: RMAN Ausnahme: ORACLE-00101: Fehler beim Ausführen des RMAN Befehls.	Die Archivprotokolldateien werden manuell aus den Speicherprotokollzielen gelöscht.	Verbinden Sie sich über den SnapManager-Host mit RMAN. Führen Sie den Befehl RMAN CROSSCHECK ARCHIVELOG ALL aus und führen Sie den Beschneiungsvorgang für die Archivprotokolldateien erneut durch.
Shell-Ausgabe konnte nicht analysiert werden: (java.util.regex.Matcher[pattern=Befehl abgeschlossen. Region=0,18 lastmatch=]) stimmt nicht überein (Name:Backup_script) Shell-Ausgabe konnte nicht analysiert werden (java.util.regex.Matcher[pattern=Befehl abgeschlossen. Region=0,25 lastmatch=]) stimmt nicht überein (Beschreibung:Sicherungsskript) Shell-Ausgabe konnte nicht analysiert werden: (java.util.regex.Matcher[pattern=Befehl abgeschlossen. Region=0,9 lastmatch=]) stimmt nicht überein (Timeout:0)	Umgebungsvariablen werden in den Skripten vor oder nach der Aufgabe nicht richtig festgelegt.	Überprüfen Sie, ob die vor- oder Nachaufgaben-Skripte der Standard-SnapManager-Plug-in-Struktur entsprechen. Weitere Informationen über die Verwendung der Umgebungsvariablen im Skript finden Sie unter Vorgänge in Taskskripten.
ORA-01450: Maximale Schlüssellänge (6398) überschritten.	Wenn Sie ein Upgrade von SnapManager 3.2 für Oracle auf SnapManager 3.3 für Oracle durchführen, schlägt der Aktualisierungsvorgang mit dieser Fehlermeldung fehl. Dieses Problem kann aus einem der folgenden Gründe auftreten: • Die Blockgröße des Tablespaces, in dem das Repository vorhanden ist, beträgt weniger als 8 KB. • der parameter nls_length_semantik wird auf char gesetzt.	Sie müssen die Werte den folgenden Parametern zuweisen: • Block_size=8192 • nls_length=Byte Nach dem Ändern der Parameterwerte müssen Sie die Datenbank neu starten. Weitere Informationen finden Sie im Knowledge Base-Artikel 2017632.

Fehlermeldungen im Zusammenhang mit dem Datenbank-Backup-Prozess (Serie 2000)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die bei der Datensicherung der Datenbank auftreten:

Fehlermeldung	Erklärung	Auflösung
SMO-02066: Sie können die Archiv-Log-Sicherung „Data-logs“ nicht löschen oder freigeben, da der Backup mit Daten-Backup „Data-logs“ verknüpft ist.	Die Sicherung des Archivprotokolls wird zusammen mit der Datensicherung der Datendateien erstellt, und Sie haben versucht, die Sicherung des Archivprotokolls zu löschen.	Verwenden Sie die Option -Force, um die Sicherung zu löschen oder zu löschen.
SMO-02067: Sie können das Archivprotokoll-Backup „Data-Logs“ nicht löschen oder freigeben, da der Backup mit der Daten-Backup „Data-Logs“ verknüpft ist und innerhalb der zugewiesenen Aufbewahrungsdauer liegt.	Die Sicherung des Archivprotokolls ist mit dem Datenbank-Backup verknüpft und befindet sich innerhalb des Aufbewahrungszeitraums, und Sie haben versucht, das Backup des Archivprotokolls zu löschen.	Verwenden Sie die Option -Force, um die Sicherung zu löschen oder zu löschen.
SMO-07142: Archivierte Protokolle werden aufgrund des Ausschlussmusters <Ausschlussmuster> Pattern ausgeschlossen.	Während der Erstellung von Profilen oder Sicherungskopien werden einige Archivprotokolldateien ausgeschlossen.	Es ist keine Aktion erforderlich.
SMO-07155: <count> archivierte Log-Dateien sind nicht im aktiven File System vorhanden. Diese archivierten Protokolldateien werden nicht in die Sicherung aufgenommen.	Die Archivprotokolldateien sind während der Erstellung von Profilen oder Backups nicht im aktiven Dateisystem vorhanden. Diese archivierten Log-Dateien sind nicht im Backup enthalten.	Es ist keine Aktion erforderlich.
SMO-07148: Archivierte Log-Dateien sind nicht verfügbar.	Während der Profilerstellung oder der Sicherungserstellung werden für die aktuelle Datenbank keine Archivprotokolldateien erstellt.	Es ist keine Aktion erforderlich.
SMO-07150: Archivierte Log-Dateien wurden nicht gefunden.	Alle Archivprotokolldateien fehlen im Dateisystem oder werden während der Erstellung von Profilen oder Backups ausgeschlossen.	Es ist keine Aktion erforderlich.

SMO-13032: Backup Create kann nicht durchgeführt werden. Ursache: ORACLE-20001: Fehler beim Versuch, Status zu ändern, um FÜR Datenbank-Instanz ZU ÖFFNEN dfcln1: ORACLE-20004: Es wird erwartet, die Datenbank ohne die RESETLOGS-Option zu öffnen, aber oracle berichtet, dass die Datenbank mit der RESETLOGS-Option geöffnet werden muss. Um das unerwartete Zurücksetzen der Protokolle zu verhindern, wird der Prozess nicht fortgesetzt. Bitte stellen Sie sicher, dass die Datenbank ohne die RESETLOGS-Option geöffnet werden kann, und versuchen Sie es erneut.	Sie versuchen, die geklonte Datenbank zu sichern, die mit der Option -no-resetlogs erstellt wurde. Die geklonte Datenbank ist keine vollständige Datenbank.Sie können jedoch SnapManager Vorgänge wie das Erstellen von Profilen und Backups, das Aufteilen von Klonen usw. mit der geklonten Datenbank ausführen, die SnapManager Vorgänge schlagen jedoch fehl, da die geklonte Datenbank nicht als vollständige Datenbank konfiguriert ist.	Stellen Sie die geklonte Datenbank wieder her, oder konvertieren Sie die Datenbank in eine Data Guard Standby Datenbank.

Datensicherungsfehler

Die folgende Tabelle zeigt häufige Fehler im Zusammenhang mit Datensicherung:

Fehlermeldung	Erklärung	Auflösung
Sicherungsschutz wird angefordert, aber das Datenbankprofil verfügt nicht über eine Schutzrichtlinie. Aktualisieren Sie die Schutzrichtlinie im Datenbankprofil oder verwenden Sie bei der Erstellung von Backups nicht die Option „schützen“.	Sie versuchen, ein Backup mit Schutz auf dem sekundären Speicher zu erstellen. Das Profil, das mit diesem Backup verknüpft ist, hat jedoch keine Schutzrichtlinie angegeben.	Bearbeiten Sie das Profil und wählen Sie eine Schutzrichtlinie aus. Erstellen Sie das Backup erneut.
Profil kann nicht gelöscht werden, da die Datensicherung aktiviert ist, der Protection Manager jedoch vorübergehend nicht verfügbar ist. Bitte versuchen Sie es später wieder.	Sie versuchen, ein Profil zu löschen, bei dem der Schutz aktiviert ist; der Protection Manager ist jedoch nicht verfügbar.	Stellen Sie sicher, dass entsprechende Backups auf primärem oder sekundärem Storage gespeichert sind. Deaktivieren Sie den Schutz im Profil. Wenn Protection Manager wieder verfügbar ist, kehren Sie zum Profil zurück und löschen Sie ihn.

Schutzrichtlinien können nicht aufgeführt werden, da Protection Manager vorübergehend nicht verfügbar ist. Bitte versuchen Sie es später wieder.	Beim Einrichten des Backup-Profils haben Sie den Schutz auf dem Backup aktiviert, sodass das Backup auf dem Sekundärspeicher gespeichert werden würde. SnapManager kann jedoch die Sicherungsrichtlinien nicht über die Protection Manager Management Console abrufen.	Deaktivieren Sie den Schutz im Profil vorübergehend. Fahren Sie mit dem Erstellen eines neuen Profils fort oder aktualisieren Sie ein vorhandenes Profil. Wenn wieder Protection Manager verfügbar ist, kehren Sie zum Profil zurück.
Sicherungsrichtlinien können nicht aufgeführt werden, da Protection Manager nicht installiert ist oder SnapDrive nicht für die Verwendung konfiguriert ist. Installieren Sie den Protection Manager und/oder konfigurieren Sie SnapDrive.	Beim Einrichten des Backup-Profils haben Sie den Schutz auf dem Backup aktiviert, sodass das Backup auf dem Sekundärspeicher gespeichert werden würde. Allerdings kann SnapManager die Sicherungsrichtlinien nicht über die Management-Konsole des Protection Manager abrufen. Der Protection Manager ist nicht installiert oder SnapDrive ist nicht konfiguriert.	Installieren Sie Protection Manager. Konfigurieren Sie SnapDrive. Kehren Sie zum Profil zurück, aktivieren Sie den Schutz erneut, und wählen Sie die Schutzrichtlinien aus, die in der Management Console von Protection Manager zur Verfügung stehen.
Schutzrichtlinie kann nicht festgelegt werden, da Protection Manager vorübergehend nicht verfügbar ist. Bitte versuchen Sie es später wieder.	Beim Einrichten des Backup-Profils haben Sie den Schutz auf dem Backup aktiviert, sodass das Backup auf dem Sekundärspeicher gespeichert werden würde. Allerdings kann SnapManager die Sicherungsrichtlinien nicht über die Management-Konsole des Protection Manager abrufen.	Deaktivieren Sie den Schutz im Profil vorübergehend. Fahren Sie mit dem Erstellen oder Aktualisieren des Profils fort. Wenn die Management Console von Protection Manager verfügbar ist, kehren Sie zum Profil zurück.
Neuer Datensatz <Dataset_Name> für Datenbank <dbname> auf Host <Host> wird erstellt.	Sie haben versucht, ein Backup-Profil zu erstellen. SnapManager erstellt für dieses Profil einen Datensatz.	Keine Aktion erforderlich.
Datensicherung ist nicht verfügbar, da Protection Manager nicht installiert ist.	Beim Einrichten des Backup-Profils haben Sie versucht, den Schutz für das Backup zu aktivieren, damit das Backup auf dem Sekundärspeicher gespeichert werden würde. Allerdings kann SnapManager nicht auf Sicherungsrichtlinien über die Management-Konsole des Protection Manager zugreifen. Der Protection Manager ist nicht installiert.	Installieren Sie Protection Manager.

Datensatz <Dataset_Name> für diese Datenbank wurde gelöscht.	Sie haben ein Profil gelöscht. SnapManager löscht den zugehörigen Datensatz.	Es ist keine Aktion erforderlich.
Das Löschen von Profilen mit aktiviertem Schutz und Protection Manager ist nicht mehr konfiguriert. Das Profil wird aus SnapManager gelöscht, der Datensatz in Protection Manager jedoch nicht gereinigt.	Sie haben versucht, ein Profil zu löschen, bei dem der Schutz aktiviert ist. Der Protection Manager ist jedoch nicht mehr installiert oder nicht mehr konfiguriert oder abgelaufen. SnapManager wird das Profil löschen, aber nicht der Datensatz des Profils aus der Managementkonsole des Protection Manager.	Installieren Sie den Protection Manager neu oder konfigurieren Sie ihn neu. Kehren Sie zum Profil zurück und löschen Sie es.
Ungültige Aufbewahrungsklasse. Verwenden Sie „smo help Backup“, um eine Liste der verfügbaren Aufbewahrungsklassen zu sehen.	Beim Einrichten der Aufbewahrungsrichtlinie haben Sie versucht, eine ungültige Aufbewahrungsklasse zu verwenden.	Erstellen Sie eine Liste gültiger Aufbewahrungsklassen durch Eingabe des Befehls: smo help Backup Aktualisieren Sie die Aufbewahrungsrichtlinie mit einer der verfügbaren Klassen.
Die angegebene Schutzrichtlinie steht nicht zur Verfügung. Eine Liste der verfügbaren Sicherungsrichtlinien finden Sie in der Liste der verfügbaren Sicherungsrichtlinien.	Beim Einrichten des Profils haben Sie den Schutz aktiviert und eine Schutzrichtlinie eingegeben, die nicht verfügbar ist.	Identifizieren Sie die verfügbaren Sicherheitsrichtlinien, indem Sie den folgenden Befehl eingeben: smo Protection-Policy list
Mit vorhandenem Datensatz <Dataset_Name> für Datenbank <dbname> auf Host <Host> da der Datensatz bereits vorhanden ist.	Sie haben versucht, ein Profil zu erstellen. Der Datensatz für dasselbe Datenbankprofil ist jedoch bereits vorhanden.	Überprüfen Sie die Optionen aus dem vorhandenen Profil, und stellen Sie sicher, dass sie mit dem übereinstimmen, was Sie im neuen Profil benötigen.
Verwenden des vorhandenen Datensatzes <Dataset_Name> für RAC-Datenbank <dbname> seit Profil <Profile_Name> für dieselbe RAC-Datenbank ist bereits vorhanden, z. B. <SID> auf Host <hostname>.	Sie haben versucht, ein Profil für eine RAC-Datenbank zu erstellen. Der Datensatz für dasselbe RAC-Datenbankprofil ist jedoch bereits vorhanden.	Überprüfen Sie die Optionen aus dem vorhandenen Profil, und stellen Sie sicher, dass sie mit dem übereinstimmen, was Sie im neuen Profil benötigen.

Für diese Datenbank ist bereits der Datensatz <Dataset_Name> mit der Schutzrichtlinie <existing_Policy_Name> vorhanden. Sie haben eine Schutzrichtlinie <New_Policy_Name> angegeben. Die Schutzrichtlinie des Datensatzes wird in <New_Policy_Name> geändert. Sie können die Schutzrichtlinie ändern, indem Sie das Profil aktualisieren.	Sie haben versucht, ein Profil mit aktiviertem Schutz und einer ausgewählten Schutzrichtlinie zu erstellen. Der Datensatz für dasselbe Datenbankprofil existiert bereits, hat aber eine andere Schutzrichtlinie. SnapManager verwendet die neu angegebene Richtlinie für den vorhandenen Datensatz.	Prüfen Sie diese Schutzrichtlinie und bestimmen Sie, ob es sich um die Richtlinie handelt, die Sie für den Datensatz verwenden möchten. Falls nicht, bearbeiten Sie das Profil und ändern Sie die Richtlinie.
Der Protection Manager löscht die lokalen Backups, die von SnapManager für Oracle erstellt wurden	Die Managementkonsole des Protection Manager löscht oder befreit die lokalen Backups, die durch SnapManager erstellt wurden, auf der Grundlage der im Protection Manager definierten Aufbewahrungsrichtlinie. Die für die lokalen Backups festgelegte Aufbewahrungsklasse wird beim Löschen oder Freigeben der lokalen Backups nicht berücksichtigt.Wenn die lokalen Backups auf ein sekundäres Speichersystem übertragen werden, werden die für die lokalen Backups auf dem primären Speichersystem festgelegten Aufbewahrungsklassen nicht berücksichtigt. Die im Übertragungsplan angegebene Aufbewahrungsklasse ist dem Remote-Backup zugewiesen.	Führen Sie den DFPM Datensatz fix_smo Befehl vom Protection Manager Server jedes Mal aus, wenn ein neuer Datensatz erstellt wird.Jetzt werden die Backups nicht basierend auf der Aufbewahrungsrichtlinie gelöscht, die in der Protection Manager Management Console eingestellt ist.

Sie möchten den Schutz für dieses Profil deaktivieren. Dies könnte potenziell den zugehörigen Datensatz in Protection Manager löschen und die für diesen Datensatz erstellten Replizierungsbeziehungen zerstören. Sie können darüber hinaus keine SnapManager Vorgänge wie beispielsweise das Wiederherstellen oder Klonen von sekundären oder tertiären Backups für dieses Profil durchführen. Möchten Sie fortfahren (J/N)?	Sie haben versucht, den Schutz für ein geschütztes Profil zu deaktivieren, während Sie das Profil von der SnapManager CLI oder GUI aktualisieren. Sie können den Schutz für das Profil mithilfe der Option -noprotect aus der SnapManager-CLI deaktivieren oder das Kontrollkästchen **Protection Manager Protection Policy** im Fenster Policies Properties über die SnapManager-Benutzeroberfläche deaktivieren. Wenn Sie den Schutz für das Profil deaktivieren, löscht SnapManager für Oracle den Datensatz aus der Management Console des Protection Manager. In dieser werden alle sekundären und tertiären Backup-Kopien, die diesem Datensatz zugeordnet sind, wieder registriert. Nach dem Löschen eines Datensatzes sind alle sekundären und tertiären Backup-Kopien verloren. Weder der Protection Manager noch der SnapManager für Oracle haben die Möglichkeit, auf diese Backup-Kopien zuzugreifen. Mithilfe von SnapManager für Oracle können die Backup-Kopien nicht mehr wiederhergestellt werden. Dieselbe Warnmeldung wird auch dann angezeigt, wenn das Profil nicht geschützt ist.	Dies ist ein bekanntes Problem in SnapManager für Oracle und erwartetes Verhalten innerhalb von Protection Manager bei der Zerstörung eines Datensatzes. Es gibt keine Problemumgehung.die verwaisten Backups müssen manuell verwaltet werden.

Fehlermeldungen im Zusammenhang mit dem Wiederherstellungsprozess (Serie 3000)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die bei der Wiederherstellung auftreten:

Fehlermeldung	Erklärung	Auflösung

SMO-03031:Restore-Spezifikation ist zur Wiederherstellung von Backup <variabel> erforderlich, da die Storage-Ressourcen für das Backup bereits freigegeben wurden.	Sie haben versucht, ein Backup wiederherzustellen, bei dem die Speicherressourcen freigegeben werden, ohne eine Wiederherstellungsspezifikation anzugeben.	Geben Sie eine Wiederherstellungsspezifikation an.
SMO-03032:Restore-Spezifikation muss Zuordnungen für die wiederherzustellenden Dateien enthalten, da die Speicherressourcen für das Backup bereits freigegeben wurden. Die Dateien, für die Zuordnungen erforderlich sind, sind: <variabel> aus Snapshots: <Variable>	Sie haben versucht, ein Backup wiederherzustellen, bei dem die Speicherressourcen entlastet wurden, und eine Wiederherstellungsspezifikation, die keine Zuordnung für alle wiederherzustellenden Dateien enthält.	Korrigieren Sie die Spezifikationsdatei für die Wiederherstellung, damit die Zuordnungen mit den wiederherzustellenden Dateien übereinstimmen.

ORACLE-30028: Protokolldatei <Dateiname> kann nicht gespeichert werden. Die Datei ist möglicherweise nicht verfügbar/nicht zugänglich/beschädigt. Diese Protokolldatei wird nicht für die Wiederherstellung verwendet.	Die Online-Redo-Log-Dateien oder Archivprotokolldateien können nicht für die Wiederherstellung verwendet werden.dieser Fehler tritt aus folgenden Gründen auf: • Die in der Fehlermeldung erwähnten Online-Redo-Log-Dateien oder archivierten Log-Dateien verfügen nicht über ausreichende Änderungsnummern, um sie für die Wiederherstellung zu beantragen. Dies geschieht, wenn die Datenbank ohne Transaktionen online ist. Das Wiederherstellungsprotokoll oder die archivierten Protokolldateien verfügen über keine gültigen Änderungsnummern, die für die Wiederherstellung angewendet werden können. • Die in der Fehlermeldung erwähnte Online-Redo-Log-Datei oder archivierte Log-Datei verfügt nicht über ausreichende Zugriffsberechtigungen für Oracle. • Die in der Fehlermeldung erwähnte Online-Redo-Log-Datei oder archivierte Log-Datei ist beschädigt und kann nicht von Oracle gelesen werden. • Die in der Fehlermeldung erwähnte Online-Protokolldatei für Wiederherstellungen oder archivierte Log-Datei wurde in dem angegebenen Pfad nicht gefunden.	Wenn es sich bei der in der Fehlermeldung genannten Datei um eine archivierte Protokolldatei handelt und wenn Sie manuell für die Wiederherstellung angegeben haben, stellen Sie sicher, dass die Datei über alle Zugriffsrechte für Oracle verfügt.selbst wenn die Datei über volle Berechtigungen verfügt, Und die Meldung wird fortgesetzt, die Archivprotokolldatei enthält keine Änderungsnummern, die für die Wiederherstellung angewendet werden müssen, und diese Meldung kann ignoriert werden.
SMO-03038: Kann keine Wiederherstellung aus dem sekundären Storage durchführen, da die Speicherressourcen weiterhin auf dem primären Volume vorhanden sind. Führen Sie stattdessen Restores von der primären aus.	Sie haben versucht, das System aus dem sekundären Storage wiederherzustellen, aber Snapshot-Kopien sind im primären Storage vorhanden.	Stellen Sie stets die Restores vom primären Speicherort wieder her, wenn das Backup nicht freigegeben wurde.

SM0-03054: Befestigung von Backup archbkp1 zur Zufuhr von Archivprotokolle. DS-10001: Anschluss von Mountpunkten. [FEHLER] FLOW-11019: Fehler in ExecuteConnectionSteps: SD-10028: SnapDrive-Fehler (id:2618 Code:305). Die folgenden Dateien konnten nicht gelöscht werden. Die entsprechenden Volumes sind möglicherweise schreibgeschützt. Wiederholen Sie den Befehl mit älteren Snapshots.[ERROR] FLOW-11010: Operation wird aufgrund eines vorherigen Fehlers abgebrochen.	Während der Wiederherstellung versucht SnapManager, das letzte Backup aus dem sekundären zu mounten, um die Archiv-Log-Dateien aus dem sekundären zu speisen.Obwohl es irgendwelche anderen Backups gibt, kann die Wiederherstellung erfolgreich sein. Aber wenn es keine anderen Backups gibt, kann die Wiederherstellung fehlschlagen.	Löschen Sie nicht die neuesten Backups aus dem primären Storage, sodass SnapManager das primäre Backup für die Recovery verwenden kann.

Fehlermeldungen, die mit dem Klonprozess verbunden sind (4000 Serie)

In der folgenden Tabelle sind die Fehler aufgeführt, die bei dem Klonprozess auftreten:

Fehlermeldung	Erklärung	Auflösung
SMO-04133: Dump-Ziel darf nicht vorhanden sein	Sie verwenden SnapManager zum Erstellen neuer Klone, jedoch sind die Dump-Ziele, die vom neuen Klon verwendet werden sollen, bereits vorhanden. SnapManager kann keinen Klon erstellen, wenn die Dump-Ziele vorhanden sind.	Entfernen oder umbenennen der alten Dump-Ziele, bevor Sie einen Klon erstellen.
SMO-04908: Kein FlexClone.	Der Klon ist ein LUN-Klon. Dies gilt für Data ONTAP 8.1 7-Mode und Clustered Data ONTAP.	SnapManager unterstützt nur die Aufteilung des Klons auf die FlexClone Technologie.
SMO-04904: Kein Klonabtrennvorgang wird mit Split-idsplit_id ausgeführt	Die Vorgangs-ID ist ungültig oder es wird kein Klon-Split-Vorgang ausgeführt.	Geben Sie eine gültige Split-ID oder Split-Bezeichnung für den Status der Clone-Split, das Ergebnis und die Stopp-Vorgänge an.
SMO-04906: Der Vorgang zum Beenden der Klonteilung ist mit Split-idsplit_id fehlgeschlagen	Der Split-Vorgang ist abgeschlossen.	Überprüfen Sie, ob der Split-Prozess derzeit ausgeführt wird, indem Sie den Befehl Clone Split-Status oder Clone Split-Ergebnis verwenden.

SMO-13032:Vorgang kann nicht ausgeführt werden: Clone Create. Ursache: ORACLE-00001: Fehler beim Ausführen von SQL: [DATENBANK ÄNDERN ÖFFNEN RESETLOGS;]. Der zurückgegebene Befehl: ORA-38856: Kann Instanz NICHT als UNNAMED_INSTANCE_2 (Redo Thread 2) als aktiviert markieren.	Die Klonerstellung schlägt fehl, wenn Sie den Klon mit dem folgenden Setup aus der Standby-Datenbank erstellen: • Die primäre Datenbank ist ein RAC Setup und die Standby-Datenbank ist Standalone. • Der Standby-Modus wird mithilfe von RMAN für das Backup der Datendateien erstellt.	Fügen Sie vor dem Erstellen des Klons den Parameter _no_Recovery_through_resetlogs= TRUE in die Klon-Spezifikations-Datei hinzu. Weitere Informationen finden Sie in der Oracle-Dokumentation (ID 334899.1). Stellen Sie sicher, dass Sie Ihren Oracle metalink-Benutzernamen und Ihr Kennwort haben.
	Sie haben in der Klon-Spezifikations-Datei keinen Wert für einen Parameter angegeben.	Sie müssen entweder einen Wert für den Parameter angeben oder diesen Parameter löschen, wenn er in der Klon-Spezifikations-Datei nicht erforderlich ist.

Fehlermeldungen im Zusammenhang mit der Verwaltung des Profilprozesses (5000-Serie)

In der folgenden Tabelle sind die Fehler aufgeführt, die bei dem Klonprozess auftreten:

Fehlermeldung	Erklärung	Auflösung
SMO-20600: Profil „profil1“ nicht im Repository "repo_Name" gefunden. Aktualisieren Sie bitte Ihre Profil-zu-Repository-Zuordnungen mit „Profile Sync“.	Der Dump-Vorgang kann nicht ausgeführt werden, wenn die Profilerstellung fehlschlägt.	Verwenden Sie den Smosystem-Dump.

Fehlermeldungen im Zusammenhang mit der Entlastung von Backup-Ressourcen (Backups 6000 Serie)

Die folgende Tabelle zeigt die häufigsten Fehler bei Backup-Aufgaben:

Fehlermeldung	Erklärung	Auflösung
SMO-06030: Backup kann nicht entfernt werden, da er in Verwendung ist: <Variable>	Sie haben versucht, den freien Vorgang für Backups mithilfe von Befehlen durchzuführen, wenn das Backup gemountet oder über Klone verfügt oder als unbegrenzt aufbewahrt werden soll.	Heben Sie die Bereitstellung des Backups auf, oder ändern Sie die Richtlinie für unbegrenzte Aufbewahrung. Sind Klone vorhanden, löschen Sie diese.

SMO-06045: Kann Backups nicht kostenlos erstellen <variabel>, da die Speicherressourcen für das Backup bereits freigegeben wurden	Sie haben versucht, den freien Vorgang des Backups über Befehle auszuführen, wenn das Backup bereits freigegeben wurde.	Sie können das Backup nicht freigeben, wenn es bereits freigegeben ist.
SMO-06047: Es können nur erfolgreiche Backups freigegeben werden. Der Status des Backups <ID> lautet <Status>.	Sie haben versucht, den kostenlosen Backup-Vorgang mithilfe von Befehlen auszuführen, wenn der Backup-Status nicht erfolgreich war.	Versuchen Sie es nach einer erfolgreichen Sicherung erneut.
SMO-13082: Vorgang kann nicht <variabel> für Backup <ID> ausgeführt werden, da die Storage-Ressourcen für das Backup freigegeben wurden.	Mit Befehlen haben Sie versucht, ein Backup bereitzustellen, das die Speicherressourcen freigegeben hat.	Sie können ein Backup, das die entsprechenden Storage-Ressourcen freigegeben hat, nicht mounten, klonen oder überprüfen.

Fehler bei der virtuellen Storage-Schnittstelle (Virtual Storage Interface 8000 Serie)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die bei Aufgaben der virtuellen Storage-Schnittstelle auftreten:

Fehlermeldung	Erklärung	Auflösung
SMO-08017 Fehler beim Erkennen des Storage für /.	SnapManager hat versucht, Speicherressourcen zu finden, fand aber Datendateien, Kontrolldateien oder Logs im Root/ Verzeichnis. Diese Dateien sollten sich in einem Unterverzeichnis befinden. Das Root-Dateisystem kann eine Festplatte in Ihrem lokalen Computer sein. SnapDrive kann an diesem Speicherort keine Snapshot Kopien erstellen, SnapManager kann keine Vorgänge für diese Dateien ausführen.	Überprüfen Sie, ob sich Datendateien, Kontrolldateien oder Wiederherstellungsprotokolle im Stammverzeichnis befinden. Wenn dies der Fall ist, verschieben Sie sie an ihre richtigen Speicherorte oder erstellen Sie Kontrolldateien oder Wiederherstellungsprotokolle an ihren richtigen Speicherorten neu. Beispiel: Verschieben Sie redo.log nach /Data/oracle/redo.log, wobei /Data/oracle der Bereitstellungspunkt ist.

Fehlermeldungen zum Rolling Upgrade-Prozess (Serie 9000)

In der folgenden Tabelle sind die häufigsten Fehler beim Rolling Upgrade aufgeführt:

Fehlermeldung	Erklärung	Auflösung

SMO-09234:die folgenden Hosts sind nicht im alten Repository vorhanden. <Hostnamen>	Sie haben versucht, ein Rolling Upgrade eines Hosts durchzuführen, der in der vorherigen Repository-Version nicht vorhanden ist.	Überprüfen Sie, ob der Host im vorherigen Repository vorhanden ist, indem Sie den Befehl Repository show-Repository aus der früheren Version der SnapManager-CLI verwenden.
SMO-09255:die folgenden Hosts sind nicht im neuen Repository vorhanden. <Hostnamen>	Sie haben versucht, ein Rollback eines Hosts durchzuführen, der in der neuen Repository-Version nicht vorhanden ist.	Überprüfen Sie, ob der Host im neuen Repository mit dem Befehl Repository show-Repository von der späteren Version der SnapManager-CLI vorhanden ist.
SMO-09256:Rollback wird nicht unterstützt, da neue Profile <Profilnamen>.für die angegebenen Hosts <Hostnamen> vorhanden sind.	Sie haben versucht, einen Host mit neuen im Repository vorhandenen Profilen wiederherzustellen. Diese Profile waren jedoch im Host der früheren SnapManager-Version nicht vorhanden.	Neue Profile in der neueren oder aktualisierten Version von SnapManager vor dem Rollback löschen.
SMO-09257:Rollback wird nicht unterstützt, da die Backups <Backupid> auf den neuen Hosts installiert sind.	Sie haben versucht, eine neuere Version des SnapManager-Hosts, der Backups gemountet hat, wiederherzustellen. Diese Backups werden in der früheren Version des SnapManager Hosts nicht eingebunden.	Heben Sie die Bereitstellung der Backups in der neueren Version des SnapManager Hosts auf, und führen Sie dann das Rollback durch.
SMO-09258:Rollback wird nicht unterstützt, da die Backups <Backupid> auf den neuen Hosts abgehängt werden.	Sie haben versucht, eine neuere Version des SnapManager-Hosts mit Backups, die nicht abgehängt werden, wiederherzustellen.	Mounten Sie die Backups in der neueren Version des SnapManager Hosts und führen Sie dann das Rollback durch.
SMO-09298:Dieses Repository kann nicht aktualisiert werden, da es bereits andere Hosts in der höheren Version hat. Führen Sie stattdessen ein RollingUpgrade für alle Hosts durch.	Sie haben ein Rolling Upgrade auf einem einzelnen Host durchgeführt und dann das Repository für diesen Host aktualisiert.	Führen Sie ein Rolling Upgrade auf allen Hosts durch.
SMO-09297: Fehler beim Aktivieren der Einschränkungen. Das Repository ist möglicherweise inkonsistent. Es wird empfohlen, das Backup des Repository, das Sie vor dem aktuellen Vorgang erstellt haben, wiederherzustellen.	Sie haben versucht, ein Rolling Upgrade oder einen Rollback-Vorgang durchzuführen, wenn die Repository-Datenbank in einem inkonsistenten Zustand bleibt.	Stellen Sie das zuvor gesicherte Repository wieder her.

Ausführung von Operationen (12,000 Serie)

In der folgenden Tabelle sind die häufigsten Fehler bei den Vorgängen aufgeführt:

Fehlermeldung	Erklärung	Auflösung
SMO-12347 [FEHLER]: SnapManager-Server wird nicht auf Host <Host> und Port <Port> ausgeführt. Führen Sie diesen Befehl auf einem Host aus, auf dem der SnapManager-Server ausgeführt wird.	Beim Einrichten des Profils haben Sie Informationen über den Host und Port eingegeben. SnapManager kann diese Vorgänge jedoch nicht ausführen, da der SnapManager-Server nicht auf dem angegebenen Host und Port ausgeführt wird.	Geben Sie den Befehl auf einem Host ein, auf dem der SnapManager-Server ausgeführt wird. Sie können den Port mit dem Befehl lsnrctl Status überprüfen und den Port anzeigen, auf dem die Datenbank ausgeführt wird. Ändern Sie bei Bedarf den Port im Backup-Befehl.

Ausführung von Prozesskomponenten (Serie 13,000)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die mit der Prozesskomponente von SnapManager verbunden sind:

Fehlermeldung	Erklärung	Auflösung
SMO-13083: Snapname-Muster mit dem Wert „x“ enthält Zeichen außer Buchstaben, Zahlen, Unterstrich, Bindestrich und geschweifte Klammern.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst. Sie haben jedoch Sonderzeichen enthalten, die nicht zulässig sind.	Entfernen Sie Sonderzeichen mit Ausnahme von Buchstaben, Zahlen, Unterstrichen, Bindestrich und geschweiften Klammern.
SMO-13084: Das Snapname-Muster mit dem Wert „x“ enthält nicht die gleiche Anzahl von linken und rechten Klammern.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst. Die linke und rechte geschweifte Klammern stimmen jedoch nicht überein.	Geben Sie im Snapname-Muster passende Öffnungs- und schließende Klammern ein.
SMO-13085: Das Snapname-Muster mit dem Wert „x“ enthält einen ungültigen Variablennamen von „y“.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst. Sie haben jedoch eine Variable enthalten, die nicht zulässig ist.	Entfernen Sie die beleidende Variable. Eine Liste der zulässigen Variablen finden Sie unter Benennen von Snapshot-Kopien.
SMO-13086 Snapname-Muster mit dem Wert „x“ muss die Variable „smid“ enthalten.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst; Sie haben jedoch die erforderliche smid-Variable weggelassen.	Geben Sie die erforderliche smid-Variable ein.

SMO-13902: Start von Clone Split ist fehlgeschlagen.	Es kann mehrere Gründe für diesen Fehler geben: • Kein Platz im Volume. • SnapDrive wird nicht ausgeführt. • Klon kann ein LUN-Klon sein. • Das FlexVol Volume verfügt über eingeschränkte Snapshot Kopien.	Überprüfen Sie mit dem Befehl „Clone Split-geschätzte“, ob im Volume genügend Speicherplatz verfügbar ist. Vergewissern Sie sich, dass der FlexVol-Volume keine eingeschränkten Snapshot-Kopien enthält.
SMO-13904: Ergebnis für Klonaufgeteilt ist fehlgeschlagen.	Dies kann auf einen Ausfall im SnapDrive oder Speichersystem zurückzuführen sein.	Versuchen Sie, an einem neuen Klon zu arbeiten.
SMO-13906: Split-Vorgang wird bereits für Clone-Label oder IDClone-ID ausgeführt	Sie versuchen, einen bereits geteilten Klon aufzuteilen.	Der Klon ist bereits aufgeteilt und die zu klonenden Metadaten werden entfernt.
SMO-13907: Split-Vorgang wird bereits für Clone-Label oder IDClone-ID ausgeführt	Sie versuchen, einen Klon aufzuteilen, der gerade den Split-Prozess durchläuft.	Sie müssen warten, bis der Splittvorgang abgeschlossen ist.

Fehlermeldungen zu SnapManager Utilities (14,000 Series)

Die folgende Tabelle zeigt die häufigsten Fehler im Zusammenhang mit SnapManager-Dienstprogrammen:

Fehlermeldung	Erklärung	Auflösung
SMO-14501: E-Mail-ID darf nicht leer sein.	Sie haben die E-Mail-Adresse nicht eingegeben.	Geben Sie eine gültige E-Mail-Adresse ein.
SMO-14502: E-Mail-Betreff darf nicht leer sein.	Sie haben den Betreff der E-Mail nicht eingegeben.	Geben Sie den entsprechenden E-Mail-Betreff ein.
SMO-14506: Das Feld für den E-Mail-Server darf nicht leer sein.	Sie haben den Hostnamen oder die IP-Adresse des E-Mail-Servers nicht eingegeben.	Geben Sie den gültigen Hostnamen oder die IP-Adresse des Mail-Servers ein.
SMO-14507: Das Feld „Mail-Port“ darf nicht leer sein.	Sie haben die E-Mail-Portnummer nicht eingegeben.	Geben Sie die Anschlussnummer des E-Mail-Servers ein.
SMO-14508: From Mail ID darf nicht leer sein.	Sie haben die E-Mail-Adresse des Absenders nicht eingegeben.	Geben Sie die E-Mail-Adresse eines gültigen Absenders ein.

SMO-14509: Benutzername darf nicht leer sein.	Sie haben die Authentifizierung aktiviert und den Benutzernamen nicht angegeben.	Geben Sie den Benutzernamen für die E-Mail-Authentifizierung ein.
SMO-14510: Das Passwort darf nicht leer sein. Geben Sie das Passwort ein.	Sie haben die Authentifizierung aktiviert und kein Passwort angegeben.	Geben Sie das E-Mail-Authentifizierungskennwort ein.
SMO-14550: E-Mail-Status <Erfolg/Ausfall>	Die Port-Nummer, der Mail-Server oder die E-Mail-Adresse des Empfängers sind ungültig.	Geben Sie bei der E-Mail-Konfiguration korrekte Werte an.
SMO-14559: Senden der E-Mail-Benachrichtigung fehlgeschlagen: <error>.	Dies kann auf eine ungültige Portnummer, einen ungültigen Mailserver oder eine ungültige E-Mail-Adresse des Empfängers zurückzuführen sein.	Geben Sie bei der E-Mail-Konfiguration korrekte Werte an.
SMO-14560: Benachrichtigung fehlgeschlagen: Die Benachrichtigungskonfiguration ist nicht verfügbar.	Senden der Benachrichtigung fehlgeschlagen, da die Benachrichtigungskonfiguration nicht verfügbar ist.	Benachrichtigungskonfiguration hinzufügen
SMO-14565: Ungültiges Zeitformat. Geben Sie das Zeitformat in HH:mm ein.	Sie haben die Uhrzeit in einem falschen Format eingegeben.	Geben Sie die Uhrzeit im Format hh:mm ein.
SMO-14566: Ungültiger Datumswert. Gültiger Datumsbereich: 1-31.	Das konfigurierte Datum ist falsch.	Das Datum muss zwischen 1 und 31 liegen.
SMO-14567: Ungültiger Tagewert. Gültiger Tagesbereich: 1-7.	Der konfigurierte Tag ist falsch.	Geben Sie den Tagesbereich zwischen 1 und 7 ein.
SMO-14569: Der Server konnte den Terminplan für die Zusammenfassung nicht starten.	Der SnapManager-Server wurde aus unbekannten Gründen heruntergefahren.	Starten Sie den SnapManager-Server.
SMO-14570: Benachrichtigung über Zusammenfassung nicht verfügbar.	Sie haben keine Übersichtsbenachrichtigung konfiguriert.	Konfigurieren Sie die zusammenfassende Benachrichtigung.
SMO-14571: Profil- und zusammenfassende Benachrichtigungen können nicht aktiviert werden.	Sie haben die Benachrichtigungsoptionen für Profil und Zusammenfassung ausgewählt.	Aktivieren Sie die Profilbenachrichtigung oder die Übersichtbenachrichtigung.

SMO-14572: Bieten Sie Erfolg- oder Fehleroption zur Benachrichtigung.	Sie haben die Erfolgs- oder Fehleroptionen nicht aktiviert.	Sie müssen entweder die Option Erfolg oder Fehler oder beides auswählen.

Allgemeine Fehlermeldungen bei SnapDrive für UNIX

Die folgende Tabelle zeigt die häufigsten Fehler im Zusammenhang mit SnapDrive für UNIX:

Fehlermeldung	Erklärung
0001-136 Admin-Fehler: Anmeldung beim Filer nicht möglich: <Filer> Bitte legen Sie den Benutzernamen und/oder das Passwort für <Filer> fest	Anfänglicher Konfigurationsfehler
0001-382 Admin-Fehler: Multipathing-Rescan fehlgeschlagen	Fehler bei der LUN-Erkennung
0001-462 Admin-Fehler: Konnte Multipathing für <LUN> nicht aufheben: Spd5: Gerät kann nicht angehalten werden. Gerät belegt.	Fehler bei der LUN-Erkennung
0001-476 Admin error: Das Gerät, das mit… verknüpft ist, kann nicht gefunden werden.	Fehler bei der LUN-Erkennung
0001-680 Admin-Fehler: Host OS erfordert ein Update auf interne Daten, um LUN-Erstellung oder Verbindung zu ermöglichen. Verwenden Sie 'SnapDrive config luns vorbereiten' oder aktualisieren Sie diese Informationen manuell…	Fehler bei der LUN-Erkennung
0001-710 Admin-Fehler: OS-Aktualisierung der LUN fehlgeschlagen…	Fehler bei der LUN-Erkennung
0001-817 Admin-Fehler: Volume-Klon konnte nicht erstellt werden… : FlexClone nicht lizenziert	Anfänglicher Konfigurationsfehler
0001-817 Admin-Fehler: Volume-Klon konnte nicht erstellt werden… : Anfrage fehlgeschlagen, da Platz für den Klon nicht garantiert werden kann.	Speicherplatzproblem
0001-878 Admin-Fehler: HBA-Assistent wurde nicht gefunden. Befehle, die LUNs betreffen, sollten fehlschlagen.	Fehler bei der LUN-Erkennung
SMO-12111: Fehler beim Ausführen des SnapDrive-Befehls „<SnapDrive Command>“: <SnapDrive Fehler>	Generischer Fehler von SnapDrive für UNIX

Verwandte Informationen

Benennen von Snapshot-Kopien

Installations- und Administrationsanleitung

Dieser Leitfaden beschreibt die Installation und Verwaltung von SnapManager 3.4.2 für Oracle in einer Windows-Umgebung, einschließlich Installation, Upgrade, Deinstallation und Konfiguration des Produkts, Backup, Wiederherstellung und Klonen von Datenbanken.

Was ist SnapManagerfür Oracle

SnapManager bietet die Tools, die für richtlinienbasiertes Datenmanagement, die Planung und Erstellung von regelmäßigen Datenbank-Backups, die Wiederherstellung von Daten aus diesen Backups im Falle von Datenverlust oder Notfällen und die Erstellung von Datenbankklonen erforderlich sind. Sie können Backups auf dem Primärspeicher erstellen und geschützte Backups auf dem Sekundärspeicher mithilfe von Post-Processing-Skripten erstellen.

SnapManager nutzt NetApp Technologien bei der Integration in die neuesten Datenbankversionen. SnapManager ist in folgende NetApp Applikationen und Technologien integriert:

- SnapDrive automatisiert Storage-Provisionierungsaufgaben und vereinfacht die Erstellung fehlerfreier und Host-konsistenter Snapshot-Kopien des Storage.
- Snapshot (eine Funktion von Data ONTAP) erstellt zeitpunktgenaue Kopien der Datenbank.
- SnapVault (eine lizenzierte Funktion von Data ONTAP) nutzt festplattenbasierte Backups für zuverlässiges Backup und Recovery von Datenbanken mit geringem Overhead.
- SnapMirror (eine lizenzierte Funktion von Data ONTAP) repliziert Datenbankdaten über ein globales Netzwerk mit hoher Geschwindigkeit auf einfache, zuverlässige und kostengünstige Weise.
- SnapRestore (eine lizenzierte Funktion von Data ONTAP) stellt eine vollständige Datenbank innerhalb weniger Sekunden wieder her – unabhängig von der Kapazität oder der Anzahl der Dateien.
- FlexClone (eine lizenzierte Funktion von Data ONTAP) hilft bei der Erstellung schneller, platzsparender Datenbankklone aus den Snapshot Backups.

SnapManager arbeitet mit SAN-Protokollen (FC und iSCSI) zusammen.

SnapManager lässt sich auch mit nativen Oracle Technologien integrieren, beispielsweise mit Oracle Recovery Manager (RMAN).

Was macht SnapManager für Oracle

SnapManager für Oracle vereinfacht und automatisiert Backups, Recoverys und das Klonen von Datenbanken mithilfe der Snapshot Kopien, SnapRestore und FlexClone Technologien.

SnapManager bietet Datenbankadministratoren (DBAs) folgende Vorteile:

- Arbeiten mit Datenbankprofilen
  - Sie können Host- und Datenbankinformationen in Profilen organisieren und aufbewahren.

Wenn Sie ein Backup auf der Grundlage eines Profils initiieren, können Sie die Informationen wiederverwenden, anstatt sie für jedes Backup erneut eingeben zu müssen. SnapManager ermöglicht Ihnen darüber hinaus die schnelle Überwachung von Abläufen mithilfe von Profilen.

  - Im Profil können Sie die Benennungsmuster für Snapshot Kopien definieren und einen benutzerdefinierten Text (Präfix oder Suffix) eingeben, sodass alle Snapshot Kopien dieselbe Namenskonvention verwenden können, die den Unternehmensrichtlinien entspricht.
  - Sie müssen den Namen des Speichersystems nicht kennen, da Datenbankdateien automatisch dem zugehörigen Speicher zugeordnet werden.
  - Wenn Sie ein neues Profil erstellen, können Sie die Option zum Trennen des Backup des Archivprotokolls von der Datensicherung der Datendatei angeben.

    Sie können das vorhandene Profil auch aktualisieren, um die Sicherung des Archivprotokolls von der Datensicherung der Datendatei zu trennen.

- Durchführen des Datenbank-Backup-Vorgangs
  - Backup von kompletten und teilweisen Datenbanken
    - Sie können schnell und platzsparend ein vollständiges oder partielles Backup erstellen, sodass Sie Backups häufiger durchführen können.

      Das vollständige Datenbank-Backup enthält alle Datendateien, Steuerdateien und Archivprotokolldateien in einem einzigen Backup.

  Das partielle Datenbank-Backup enthält bestimmte Datendateien oder Tablespaces, alle Kontrolldateien und alle Archivprotokolldateien.

  - Backups können durch Nachverarbeitungsskripte auf den Sekundärspeicher gesichert werden.
  - Die Backups können auf Stundenbasis, wöchentlich, täglich, monatlich oder unbegrenzt geplant werden.
    - Separate Backup von Datendateien und Archivprotokolldateien
  - Mit SnapManager (3.2 oder höher) können Sie die Datendateien und die Log-Dateien zur Archivierung separat sichern. Um diesen Vorgang durchzuführen, müssen Sie die Option zum Trennen der Archivprotokolldateien beim Erstellen oder Aktualisieren des Profils angeben.
  - Sie können in der Aufbewahrungsrichtlinie die Anzahl und die Dauer angeben, für die die Backups der Datendateien aufbewahrt werden sollen.
  - Sie können die Dauer für die Backups der Archivprotokolldatei angeben, die während der Aufbewahrungsdauer des Archivprotokolls aufbewahrt werden soll.
  - SnapManager (3.2 oder höher) konsolidiert außerdem die Archiv-Log-Backups auf eine Mindestanzahl von Backups, indem die Archiv-Log-Backups mit doppelten Archivprotokolldateien freigegeben werden und nur die Archiv-Log-Backups mit einzigartigen Archiv-Log-Dateien vorgehalten werden. Diese Konsolidierung kann jedoch optional deaktiviert werden.
- Verwalten der Archivprotokolldateien
  - Mit SnapManager (3.2 oder höher) können Sie die Archivprotokolldateien aus den Archivprotokollzielen beschneiden.

    Der von den beschnitten Archivprotokolldateien belegte Speicherplatz wird freigegeben, wenn die Archiv-Log-Backups, die diese Archivprotokolldateien enthalten, gelöscht werden.

  - SnapManager stellt sicher, dass die Archiv-Log-Dateien gesichert werden, bevor sie von den Archiv-

Protokollzielen beschnitten werden.

Die nicht gesicherten Archivprotokolldateien werden nicht beschnitten.

- SnapManager stellt sicher, dass die Archivprotokolldateien an die Data Guard-Standby-Datenbank gesendet werden, während Archivprotokolldateien aus einer primären Data Guard-Datenbank beschnitten werden.
- SnapManager stellt sicher, dass die Archivprotokolldateien vom Oracle Stream Capture-Prozess erfasst werden, falls vorhanden.
- Empfehlung
  - Um den Zielplatz für Archivprotokolle effektiv zu managen, müssen Sie die Archiv-Log-Backups erstellen und die Archiv-Log-Dateien damit beschneiden.
- SnapManager konsolidiert die Archiv-Log-Backups und enthält so eine Mindestanzahl von Backups, indem die Archiv-Log-Backups mit duplizierten Archiv-Log-Dateien erstellt und nur die Archiv-Log-Backups genutzt werden.

  Diese Konsolidierung kann jedoch optional deaktiviert werden. Die Archiv-Log-Backups, die doppelte Archiv-Log-Dateien enthalten, werden freigegeben und ein einzelnes Backup mit einzigartigen Archiv-Logs bleibt erhalten.

- Durchführen des Datenbankwiederherstellungsvorgangs
  - Sie können dateibasierte Restore-Vorgänge durchführen.

    Sie können außerdem eine Vorschau der Wiederherstellungsvorgänge anzeigen und eine Datei-für-Datei-Analyse von Wiederherstellungsvorgängen erhalten, bevor der Vorgang ausgeführt wird.

  - Mit SnapRestore lässt sich der mittlere Zeitaufwand für die Wiederherstellung einer Datenbank verringern.
  - Mit SnapManager (3.2 oder höher) können Sie die Datenbank automatisch wiederherstellen, indem Sie die Archivprotokolldateien aus dem Backup verwenden, selbst wenn die Archivprotokolldateien nicht im Archivprotokollziel verfügbar sind.

    SnapManager (3.2 oder höher) bietet auch eine Möglichkeit, die Datenbank durch die Verwendung der Archiv-Log-Dateien aus dem externen Standort in einem bestimmten Ausmaß wiederherzustellen.

- Klonen von Datenbanken für Tests und Entwicklung
  - Sie können einen Klon einer Datenbank erstellen, sodass die Datenbank außerhalb der Produktionsumgebung eingerichtet werden kann.

    Sie können beispielsweise in der Entwicklungs- und Testumgebung zum Testen von Upgrades auf wichtige Systeme klonen.

  - Sie können eine Datenbank auf einem Primärspeichersystem klonen.
  - Mit SnapManager (3.2 oder höher) können Sie die Backups der Datendatei mit den im Backup verfügbaren Archivprotokolldateien klonen.
    - Sie können die Backups der Datendatei nur klonen, wenn das Archivprotokoll-Backup miterstellt wird.
    - Sie können die Backups der Datendatei auch klonen, wenn die Archivprotokolldateien in einem bestimmten Umfang separat erstellten Archiv-Log-Backups zur Verfügung stehen.
    - Sie können die Backups einer eigenständigen Datenbank in einem bestimmten Umfang auch mit

Archivprotokolldateien von jedem externen Standort aus klonen, auf den Oracle zugreifen kann.

        - Wenn die Backups von einem externen Standort aus verfügbar sind, können Sie den externen Standort beim Klonen angeben, um die geklonte Datenbank in einen konsistenten Status wiederherzustellen.
    - Das Klonen der rein archivprotokollbasierten Backups wird nicht unterstützt.
- Allgemein
    - Integration mit vorhandenen Oracle Tools wie Recovery Manager (RMAN)

SnapManager bietet Storage-Administratoren folgende Vorteile:

- Unterstützt unterschiedliche SAN-Protokolle
- Ermöglicht Ihnen die Optimierung von Backups auf der Grundlage der für Ihre Umgebung am besten geeigneten Backup-Art (vollständig oder teilweise).
- Erstellt platzsparende Datenbank-Backups.
- Erstellung platzsparender Klone:

SnapManager arbeitet darüber hinaus mit folgenden Oracle Funktionen zusammen:

- SnapManager kann die Backups mit RMAN von Oracle katalogisieren.

  Bei Verwendung von RMAN kann ein DBA die SnapManager Backups nutzen und den Nutzen aller RMAN Funktionen, wie etwa das Restore auf Blockebene, erhalten. Dank SnapManager kann RMAN die Snapshot Kopien bei Recovery- oder Restore-Vorgängen verwenden. So können Sie beispielsweise RMAN zum Wiederherstellen einer Tabelle in einem Tablespace und zum Durchführen vollständiger Restores und Recoverys von Datenbanken und Tablespaces aus Snapshot-Kopien von SnapManager verwenden. Der RMAN-Wiederherstellungskatalog sollte sich nicht in der Datenbank befinden, die gesichert wird.

Integration in andere Applikationen und Technologien von NetApp

SnapManager für Oracle ist ein eigenständiges Produkt, das die Funktionen anderer NetApp Produkte integriert und so schnelle Backups ermöglicht, die nur wenig Speicherplatz benötigen.

SnapManager lässt sich mit den folgenden NetApp Applikationen und Technologien integrieren:

Anwendungen und Technologien	Beschreibung
SnapDrive	SnapManager erstellt mithilfe von SnapDrive Snapshot Kopien des Storage. Snapshot-Kopien sorgen dafür, dass Backups platzsparend und schneller erstellt werden können als die Disk-to-Disk-Backups.
FlexClone (eine lizenzierte Funktion von Data ONTAP)	SnapManager erstellt mithilfe der FlexClone Funktion schnelle, platzsparende Klone von Backups.
Snapshot (eine Funktion von Data ONTAP)	Mit der Snapshot Technologie werden zeitpunktgenaue Kopien der Datenbank erstellt.

SnapRestore (eine lizenzierte Funktion von Data ONTAP)	SnapManager reduziert mit SnapRestore die durchschnittliche Zeit zum Recovery einer Datenbank. SnapRestore kann einzelne Dateien auf einem Volume mit mehreren Terabyte wiederherstellen, sodass der Betrieb schnell wieder aufgenommen werden kann.
SnapVault (eine lizenzierte Funktion von Data ONTAP)	SnapVault nutzt festplattenbasierte Backups für zuverlässiges Backup und Recovery von Datenbanken mit geringem Overhead.
SnapMirror (eine lizenzierte Funktion der Data ONTAP)	SnapMirror repliziert Datenbankdaten einfach, zuverlässig und kostengünstig über ein globales Netzwerk mit hoher Geschwindigkeit.

Vorteile von SnapManager

Mit SnapManager für Oracle können Sie verschiedene Aufgaben an den Datenbanken ausführen und Daten effizient managen.

SnapManager für Oracle arbeitet mit Storage-Systemen zusammen und ermöglicht die folgenden Aufgaben:

- Erstellen Sie platzsparende Backups auf primärem oder sekundärem Storage und planen Sie Backups.

  Sie können vollständige und teilweise Datenbank-Backups erstellen und Richtlinien für die Aufbewahrungsdauer anwenden.SnapManager (3.2 oder höher) ermöglicht Ihnen, nur die Datendateien und Archivprotokolle zu erstellen.

  - SnapManager (3.2 oder höher) ermöglicht die Vorverarbeitung bzw. Nachbearbeitung der Backup- und Restore-Vorgänge vor oder nach der Durchführung.
  - SnapManager (3.2 oder höher) ermöglicht Ihnen den Schutz von Backups mithilfe der Nachbearbeitungsskripte.
- Stellen Sie vollständige oder teilweise Datenbanken mithilfe des dateibasierten Wiederherstellungsvorgangs wieder her.
- Automatisches Wiederherstellen und Wiederherstellen von Datenbank-Backups.

  SnapManager (3.2 oder höher) ermöglicht die automatische Wiederherstellung und Wiederherstellung von Datenbank-Backups. SnapManager stellt die wiederhergestellte Datenbank automatisch wieder her, indem die Archiv-Log-Dateien aus den Backups erkannt, Mounten und angewendet werden.
- Bei der Erstellung von Backups nur für die Archivprotokolle Archivprotokolldateien aus den Archivprotokollzielen abschneiden.
- Bewahren Sie die minimale Anzahl von Backups für Archivprotokolle automatisch auf, indem Sie nur die Backups mit einzigartigen Archivprotokolldateien aufbewahren.
- Verfolgen Sie die Betriebsdetails und erstellen Sie Berichte nach Host, Profil, Backup oder Klon.
- Überprüfen Sie den Backup-Status.
- Historie der einem Profil zugehörigen SnapManager Vorgänge beibehalten
- Erstellung platzsparender Backup-Klone auf dem Primärspeicher

Backups mit Snapshot Kopien erstellen

SnapManager ermöglicht die Erstellung von Backups auf dem primären (lokalen) Storage und auch auf dem sekundären (Remote-) Storage mithilfe von Nachbearbeitungsskripten.

Als Snapshot-Kopien erstellte Backups sind virtuelle Kopien der Datenbank und werden auf demselben physischen Medium wie die Datenbank gespeichert. Der Backup-Vorgang dauert daher weniger Zeit und erfordert deutlich weniger Speicherplatz als vollständige Disk-to-Disk Backups. Mit SnapManager können Sie Folgendes sichern:

- Alle Datendateien, archivierte Log-Dateien und Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces, alle Archivprotokolldateien und Kontrolldateien

Mit SnapManager 3.2 oder höher können Sie optional folgende Daten sichern:

- Alle Datendateien und die Kontrolldateien
- Ausgewählte Datendateien oder Tablespaces zusammen mit den Kontrolldateien
- Archivierung von Protokolldateien

Die Datendateien, Archiv-Log-Dateien und Kontrolldateien können auf verschiedenen Storage-Systemen, Storage-System-Volumes oder LUNs (Logical Unit Numbers) abgelegt werden. Sie können SnapManager auch zum Backup einer Datenbank verwenden, wenn sich mehrere Datenbanken auf demselben Volume oder LUN befinden.

Warum sollten Sie Archiv Log-Dateien beschneiden

Mit SnapManager für Oracle können Sie Archivprotokolldateien aus dem aktiven, bereits gesicherten Dateisystem löschen.

Durch Beschneidung kann SnapManager Backups einzelner Archiv-Log-Dateien erstellen. Durch Beschneidung und die Richtlinie zur Aufbewahrung von Backups wird beim Säuberen von Backups der Speicherplatz für das Archiv-Protokoll freigegeben.

Sie können die Archivprotokolldateien nicht beschneiden, wenn der Flash Recovery Area (FRA) für Archivprotokolldateien aktiviert ist. Wenn Sie im Bereich Flash Recovery den Speicherort für das Archivprotokoll angeben, müssen Sie im Parameter Archive_log_dest auch den Speicherort für das Archivprotokoll angeben.

Konsolidierung von Archivierungsprotokolldaten

Mit SnapManager (3.2 oder höher) für Oracle werden die Archiv-Log-Backups konsolidiert, um eine Mindestanzahl an Backups für Archivierungs-Log-Dateien beizubehalten. SnapManager für Oracle erkennt und befreit die Backups, die Archivprotokolle enthalten, die Teilmengen anderer Backups sind.

Vollständige oder teilweise Wiederherstellung von Datenbanken

SnapManager bietet die Flexibilität, komplette Datenbanken, bestimmte Tabellen, Dateien, Kontrolldateien oder eine Kombination dieser Einheiten wiederherzustellen. SnapManager ermöglicht die Wiederherstellung von Daten mithilfe eines dateibasierten

Wiederherstellungsprozesses.

SnapManager ermöglicht Datenbankadministratoren (DBAs) die Vorschau von Restore-Vorgängen. Mit der Vorschaufunktion können DBAs jeden Wiederherstellungsvorgang auf Datei-für-Datei-Basis anzeigen.

Datenbankadministratoren können das Level angeben, auf das SnapManager bei der Durchführung von Restore-Vorgängen wiederhergestellt und Informationen wiederhergestellt werden. Beispielsweise können DBAs Daten zu bestimmten Zeitpunkten wiederherstellen. Der Wiederherstellungspunkt kann ein Datum und eine Uhrzeit oder eine Oracle System Change Number (SCN) sein.

Datenbankadministratoren können die Datenbank mit SnapManager wiederherstellen und ein anderes Tool verwenden, um die Informationen wiederherzustellen. DBAs müssen für beide Vorgänge keine SnapManager verwenden.

Mit SnapManager (3.2 oder höher) können Datenbank-Backups automatisch und ohne Eingriff des Datenbankadministrators wiederhergestellt werden. Sie können SnapManager verwenden, um Backups für Archivprotokolle zu erstellen und dann diese Backups für Archivprotokolle zu verwenden, um die Datenbank-Backups wiederherzustellen und wiederherzustellen. Selbst wenn die Archivprotokolldateien des Backups in einem externen Archivprotokoll verwaltet werden, können Sie diesen externen Speicherort angeben, damit diese Archivprotokolle zur Wiederherstellung der wiederhergestellten Datenbank beitragen können.

Überprüfen des Backup-Status

SnapManager kann die Integrität des Backups mithilfe von standardmäßigen Oracle-Backup-Verifizierungsvorgängen bestätigen.

Datenbankadministratoren (DBAs) können die Verifizierung im Rahmen des Backup-Vorgangs oder einer anderen Zeit durchführen. Datenbankadministratoren können den Verifizierungsvorgang so einstellen, dass er bei geringerer Auslastung des Host-Servers oder während eines geplanten Wartungsfensters ausgeführt wird.

Datenbank-Backup-Klone

SnapManager erstellt mithilfe der FlexClone Technologie einen beschreibbaren, platzsparenden Klon eines Datenbank-Backups. Sie können einen Klon ändern, ohne die Backup-Quelle zu ändern.

Möglicherweise möchten Sie Datenbanken klonen, um Tests oder Upgrades in nicht produktiven Umgebungen zu ermöglichen. Sie können eine Datenbank auf dem Primärsystem klonen. Ein Klon kann sich auf demselben Host oder einem anderen Host befinden wie die Datenbank.

Mit der FlexClone Technologie können SnapManager Snapshot-Kopien der Datenbank verwenden, sodass keine vollständige physische Disk-to-Disk-Kopie erstellt werden muss. Snapshot Kopien benötigen weniger Erstellungszeit und belegen deutlich weniger Speicherplatz als physische Kopien.

In der Data ONTAP Dokumentation finden Sie weitere Informationen zur FlexClone Technologie.

Verwandte Informationen

"Data ONTAP documentation: mysupport.netapp.com/documentation/productsatoz/index.html"

Verfolgen Sie die Details und erstellen Sie Berichte

SnapManager bietet nicht nur detaillierte Datenbankadministratoren, die den Status verschiedener Vorgänge verfolgen müssen, sondern mithilfe von Methoden, die Vorgänge über eine einheitliche Benutzeroberfläche überwachen.

Nachdem Administratoren festlegen, welche Datenbanken gesichert werden sollen, identifiziert SnapManager die Datenbankdateien für das Backup automatisch. SnapManager zeigt Informationen zu Repositorys, Hosts, Profilen, Backups und Klonen an. Sie können die Vorgänge auf bestimmten Hosts oder Datenbanken überwachen.

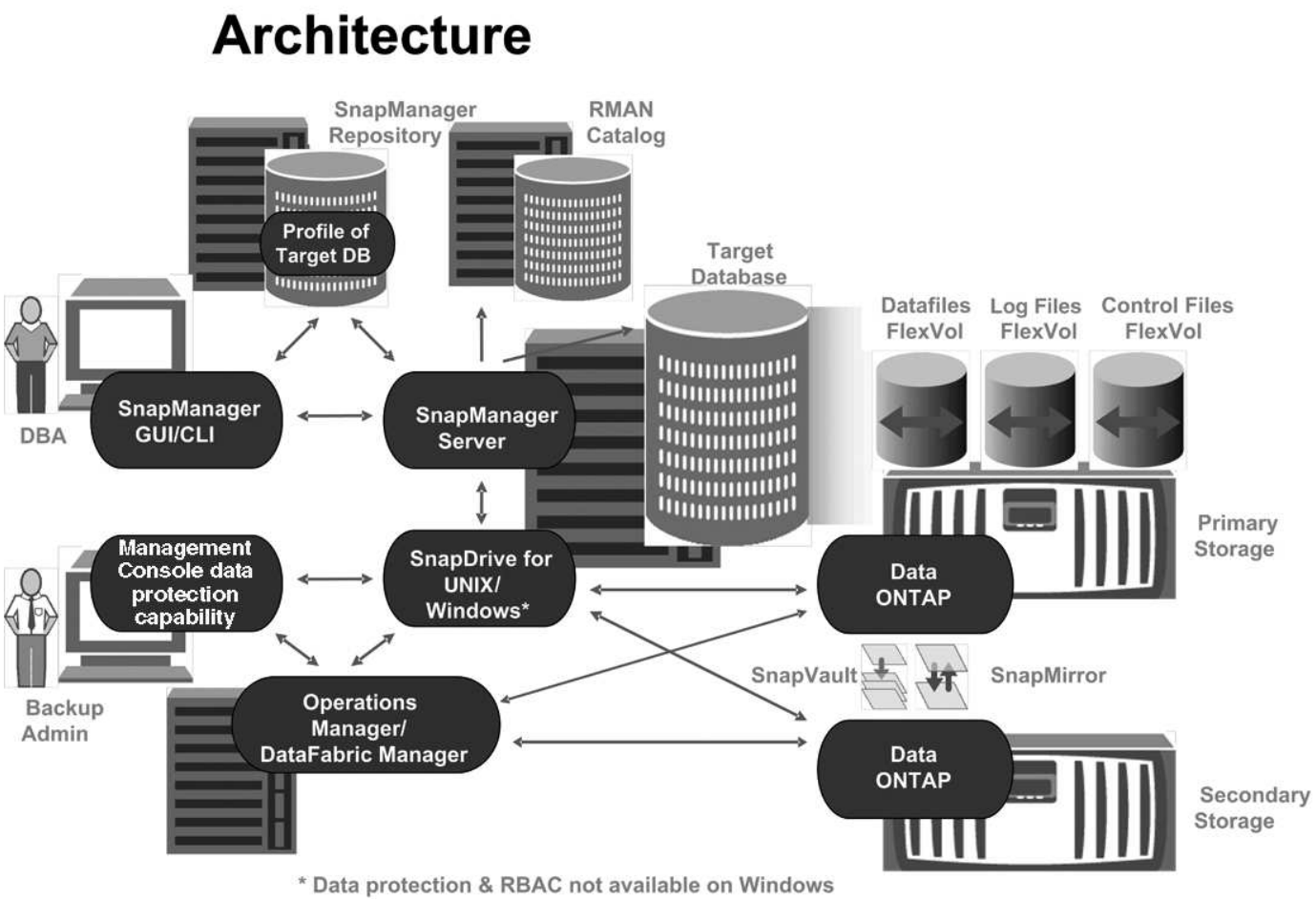
Die Architektur von SnapManager für Oracle ist das

Die Architektur von SnapManager für Oracle umfasst viele Komponenten, wie beispielsweise das SnapManager für Oracle Host, Client und Repository. Weitere Komponenten sind die primären und sekundären Storage-Systeme und andere NetApp Produkte.

Die Architektur von SnapManager für Oracle umfasst die folgenden Komponenten:

- SnapManager Host
- Grafische SnapManager Benutzeroberfläche oder Befehlszeilenschnittstelle
- SnapManager Repository
- Primärspeicher
- Sekundäre Storage-Systeme
- SnapDrive für Windows

Das folgende Bild zeigt die Architektur von SnapManager für Oracle sowie die zugehörigen Komponenten:



SnapManager Host

Der SnapManager Host ist ein Windows Server, der auch andere NetApp Produkte ausführt.

Der SnapManager Host wird mit den folgenden Produkten installiert:

- SnapDrive für Windows
- Host Utilities

Der SnapManager-Host wird als Service ausgeführt.

Grafische SnapManager-Benutzer- und Befehlszeilenschnittstellen

Der SnapManager Client enthält eine grafische Benutzeroberfläche (GUI) und eine Befehlszeilenschnittstelle (CLI).

SnapManager Repository

Im Repository werden Informationen zu verschiedenen SnapManager-Vorgängen gespeichert, beispielsweise die Zeit von Backups, Tabellen und Datendateien, die gesichert wurden, bei Storage-Systemen, bei erstellten Klonen und bei Snapshot Kopien.

Die Repository-Datenbank kann nicht in derselben Datenbank vorhanden sein und darf auch nicht Teil

derselben Datenbank sein, die von SnapManager gesichert wird. Dies liegt daran, dass das Repository die Namen der Datenbank-Snapshot-Kopien speichert, die während des Backup-Betriebs erstellt wurden. Das Repository muss in einer anderen Datenbank als der zu sichernden Datenbank erstellt werden. Das heißt, Sie müssen mindestens zwei Datenbanken haben: Die SnapManager Repository-Datenbank und die von SnapManager gemanagte Zieldatenbank. Wenn Sie die SnapManager-Services ausführen, müssen beide Datenbanken betriebsbereit sein.

SnapManager-Vorgänge dürfen nicht über die GUI oder die CLI ausgeführt werden, wenn die Repository-Datenbank ausfällt.

SnapDrive auf SnapManager Server

SnapManager erstellt Snapshot Kopien des Storage-Systems mithilfe von SnapDrive für Windows. SnapDrive befindet sich auf demselben Server wie SnapManager.

Repositories

SnapManager organisiert die Informationen in Profile, die dann den Repositories zugeordnet werden. Profile enthalten Informationen über die zu verwaltende Datenbank, während das Repository Daten zu den Vorgängen enthält, die auf Profilen ausgeführt werden.

Das Repository zeichnet auf, wann ein Backup durchgeführt wurde, welche Dateien gesichert wurden und ob ein Klon aus dem Backup erstellt wurde. Wenn Datenbankadministratoren eine Datenbank wiederherstellen oder einen Teil davon wiederherstellen, fragt SnapManager das Repository ab, um zu ermitteln, was gesichert wurde.

Da das Repository die Namen der während des Backup erstellten Datenbank-Snapshot-Kopien speichert, kann die Repository-Datenbank nicht in derselben Datenbank vorhanden sein und kann auch nicht Teil derselben Datenbank sein, die von SnapManager gesichert wird. Sie müssen mindestens zwei Datenbanken (die SnapManager Repository-Datenbank und die von SnapManager gemanagte Zieldatenbank) einrichten und ausführen, wenn Sie SnapManager Vorgänge ausführen.

Wenn Sie versuchen, die grafische Benutzeroberfläche (GUI) zu öffnen, wenn die Repository-Datenbank nicht verfügbar ist, wird die folgende Fehlermeldung in der Datei sm_gui.log protokolliert: [WARNUNG]: SMO-01106: Beim Abfragen des Repository ist ein Fehler aufgetreten: Keine Daten mehr aus dem Socket zu lesen. Außerdem schlägt das SnapManager-Verfahren fehl, wenn die Repository-Datenbank ausfällt. Weitere Informationen zu den verschiedenen Fehlermeldungen finden Sie unter *Fehlerbehebung bekannter Probleme*.

Sie können jeden beliebigen Host-Namen, Dienstnamen oder Benutzernamen verwenden, um Vorgänge auszuführen. Damit ein Repository SnapManager-Vorgänge unterstützt, müssen der Projektarchiv-Benutzername und der Dienstname nur aus den folgenden Zeichen bestehen: Alphabetische Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-), Unterstrich (_) und Punkt (.).

Der Repository-Port kann eine beliebige gültige Portnummer sein, und der Repository-Hostname kann einen beliebigen gültigen Hostnamen sein. Der Hostname muss aus alphabetischen Zeichen (A-Z), Ziffern (0-9), Minuszeichen (-) und Periode (.) bestehen, jedoch nicht aus einem Unterstrich (_).

Das Repository muss in einer Oracle-Datenbank erstellt werden. Die von SnapManager verwendete Datenbank sollte gemäß den Oracle Verfahren für die Datenbankkonfiguration eingerichtet werden.

Ein einziges Repository kann Informationen über mehrere Profile enthalten, jedoch ist jede Datenbank normalerweise nur mit einem Profil verknüpft. Sie können mehrere Repositorys haben, wobei jedes Repository

mehrere Profile enthält.

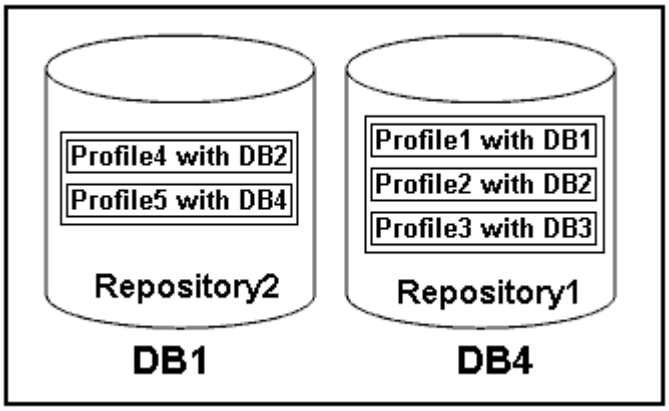
Welche Profile sind

SnapManager verwendet Profile, um die zur Durchführung von Operationen in einer bestimmten Datenbank erforderlichen Informationen zu speichern. Ein Profil enthält die Informationen zur Datenbank einschließlich aller Anmeldeinformationen, Backups und Klone. Wenn Sie ein Profil erstellen, müssen Sie keine Datenbankdetails angeben, wenn Sie eine Operation in dieser Datenbank ausführen.

Ein Profil kann nur auf eine Datenbank verweisen. Auf dieselbe Datenbank kann mit mehr als einem Profil verwiesen werden. Auf Backups, die mit einem Profil erstellt werden, kann nicht über ein anderes Profil zugegriffen werden, auch wenn beide Profile auf dieselbe Datenbank verweisen.

Profilinformationen werden in einem Repository gespeichert. Das Repository enthält sowohl die Profilinformationen für die Datenbank als auch Informationen zu den Snapshot-Kopien, die als Datenbank-Backup dienen. Die tatsächlichen Snapshot Kopien werden im Storage-System gespeichert. Die Namen der Snapshot Kopie werden im Repository gespeichert, das das Profil für diese Datenbank enthält. Wenn Sie einen Vorgang in einer Datenbank ausführen, müssen Sie das Profil aus dem Repository auswählen.

Die folgende Abbildung zeigt, wie Repositories mehrere Profile aufnehmen können, aber auch dass jedes Profil nur eine Datenbank definieren kann:



Im vorhergehenden Beispiel befindet sich Repository2 auf Datenbank DB1 und Repository1 befindet sich auf der Datenbank DB4.

Jedes Profil enthält die Anmeldeinformationen für die Datenbank, die mit dem Profil verknüpft ist. Mit den Anmeldeinformationen kann SnapManager eine Verbindung zur Datenbank herstellen und mit der Datenbank arbeiten. Die gespeicherten Anmeldeinformationen umfassen den Benutzernamen und die Kennwortpaare für den Zugriff auf den Host, das Repository, die Datenbank und die erforderlichen Verbindungsinformationen, wenn Sie Oracle Recovery Manager (RMAN) verwenden.

Sie können nicht auf ein Backup zugreifen, das mit einem Profil aus einem anderen Profil erstellt wurde, auch wenn beide Profile mit derselben Datenbank verknüpft sind. SnapManager legt eine Sperre auf die Datenbank ab, um zu verhindern, dass zwei inkompatible Vorgänge gleichzeitig ausgeführt werden.

Profil zur Erstellung vollständiger und partieller Backups

Sie können Profile erstellen, um vollständige Backups oder partielle Backups zu erstellen.

Die Profile, die Sie zur Erstellung der vollständigen und partiellen Backups angeben, enthalten sowohl die

Datendateien als auch die Archivprotokolldateien. SnapManager erlaubt solche Profile nicht, die Backups des Archivprotokolls von den Backups der Datendatei zu trennen. Die vollständigen und teilweisen Backups werden gemäß den bestehenden Richtlinien zur Backup-Aufbewahrung aufbewahrt. Sie können vollständige und teilweise Backups basierend auf der zu Ihnen passt Uhrzeit und Häufigkeit planen.

Profile für die Erstellung von datenbasierten Backups und nur-Archiv-Backups

Mit SnapManager (3.2 oder höher) können Sie Profile erstellen, die Backups der Archivprotokolldateien getrennt von den Datendateien machen. Nachdem Sie das Profil zur Trennung der Backup-Typen verwendet haben, können Sie entweder Datendateien-only-Backups oder lediglich Archiv-Log-Backups der Datenbank erstellen. Sie können auch ein Backup erstellen, das sowohl die Datendateien als auch die Archivprotokolldateien enthält.

Die Aufbewahrungsrichtlinie gilt für alle Datenbank-Backups, wenn die Archiv-Log-Backups nicht getrennt sind. Nachdem Sie die Archiv-Log-Backups getrennt haben, können Sie mit SnapManager unterschiedliche Aufbewahrungszeiten festlegen.

Aufbewahrungsrichtlinie

SnapManager legt fest, ob ein Backup aufbewahrt werden soll, indem sowohl die Anzahl der Aufbewahrung (z. B. 15 Backups) als auch die Aufbewahrungsdauer (z. B. 10 Tage tägliche Backups) berücksichtigt werden. Ein Backup läuft ab, wenn sein Alter die für seine Aufbewahrungsklasse festgelegte Aufbewahrungsdauer überschreitet und die Anzahl der Backups die Anzahl der Backups übersteigt. Beispiel: Wenn die Backup-Anzahl 15 beträgt (was bedeutet, dass SnapManager 15 erfolgreiche Backups erstellt hat) und die Dauer für tägliche Backups von 10 Tagen festgelegt wurde, verfallen die fünf ältesten, erfolgreichen und infrage kommenden Backups.

Aufbewahrungsdauer des Archivprotokolls

Nach Trennung der Backup-Protokolle werden sie basierend auf der Aufbewahrungsdauer des Archivprotokolls aufbewahrt. Backups von Archivprotokolldateien, die mit Backups von Datendateien erstellt werden, werden immer zusammen mit Backups dieser Datendateien aufbewahrt, unabhängig von der Aufbewahrungsdauer für das Archivprotokoll.

Verwandte Informationen

Profilverwaltung für effiziente Backups

Die Status der SnapManager-Operation lauten

SnapManager-Vorgänge (Backup, Wiederherstellung und Klon) können den jeweiligen Status aufweisen, wobei jeder Status den Fortschritt des Vorgangs angibt.

Betriebsstatus	Beschreibung
Erfolgreich	Die Operation wurde erfolgreich abgeschlossen.
Wird Ausgeführt	Der Vorgang wurde gestartet, ist aber noch nicht abgeschlossen. Ein Backup, das zwei Minuten dauert, wird beispielsweise um 11:00 Uhr morgens erstellt. Wenn Sie die Registerkarte **Zeitplan** um 11:01 Uhr aufrufen, wird der Vorgang als ausgeführt angezeigt.

Kein Vorgang gefunden	Der Zeitplan wurde nicht ausgeführt oder das letzte Backup wurde gelöscht.
Fehlgeschlagen	Der Vorgang ist fehlgeschlagen. SnapManager hat den Abbruchvorgang automatisch ausgeführt und den Vorgang bereinigt.

Wiederherstellbare und nicht wiederherstellbare Ereignisse

Ein wiederherstellbares SnapManager Ereignis hat die folgenden Probleme:

- Die Datenbank wird nicht auf einem Storage-System gespeichert, auf dem Data ONTAP ausgeführt wird.
- SnapDrive für Windows ist nicht installiert oder kann nicht auf das Speichersystem zugreifen.
- SnapManager erstellt keine Snapshot Kopie bzw. stellt keinen Storage bereit, wenn das Volume über keinen freien Speicherplatz verfügt, die maximale Anzahl an Snapshot Kopien erreicht oder eine unerwartete Ausnahme auftritt.

Wenn ein wiederherstellbares Ereignis eintritt, wird SnapManager abgebrochen und versucht, den Host, die Datenbank und das Storage-System auf den Startstatus zurückzusetzen. Schlägt der Abbruchvorgang fehl, behandelt SnapManager den Vorfall als nicht wiederherstellbares Ereignis.

Wenn eines der folgenden Ereignisse eintritt, tritt ein nicht behebbares (Out-of-Band)-Ereignis auf:

- Ein Systemproblem tritt auf, z. B. wenn ein Host ausfällt.
- Der SnapManager-Prozess wird angehalten.
- Der Abbruch innerhalb des Band schlägt fehl, wenn das Speichersystem ausfällt, die Nummer der logischen Einheit (LUN) oder das Speichervolume offline ist oder das Netzwerk ausfällt.

Wenn ein nicht behebbares Ereignis eintritt, wird SnapManager sofort abgebrochen. Der Host, die Datenbank und das Speichersystem sind möglicherweise nicht an den ursprünglichen Status zurückgekehrt. In diesem Fall müssen Sie nach Ausfall des SnapManager-Vorgangs eine Bereinigung durchführen, indem Sie die verwaiste Snapshot Kopie löschen und die SnapManager-Sperrdatei entfernen.

Wenn Sie die SnapManager-Sperrdatei löschen möchten, navigieren Sie auf dem Zielcomputer zu Oracle_HOME €und löschen Sie die Datei SM_Lock_TargetDBName. Nach dem Löschen der Datei müssen Sie den SnapManager für Oracle-Server neu starten.

Wie SnapManager die Sicherheit gewährleistet

Sie können SnapManager Vorgänge nur ausführen, wenn Sie die entsprechenden Anmeldedaten besitzen. Die Sicherheit in SnapManager unterliegt der Benutzerauthentifizierung.

SnapManager gewährleistet die Sicherheit, indem die Benutzerauthentifizierung über Passworteinforderungen oder durch Festlegen von Benutzeranmeldeinformationen angefordert wird. Ein effektiver Benutzer wird beim SnapManager-Server authentifiziert und autorisiert.

Die SnapManager Anmeldedaten und die Benutzerauthentifizierung unterscheiden sich erheblich von SnapManager 3.0:

- In SnapManager-Versionen vor 3.0 würden Sie bei der Installation von SnapManager ein willkürliches Serverkennwort festlegen. Wer den SnapManager-Server nutzen möchte, braucht das SnapManager-Server-Passwort. Das SnapManager-Server-Passwort muss den Benutzeranmeldeinformationen mit dem smo-Befehl „set-serm“ hinzugefügt werden.
- In SnapManager (3.0 und höher) wurde das SnapManager-Serverpasswort durch die Authentifizierung des individuellen Betriebssystems (OS) ersetzt. Wenn Sie den Client nicht vom selben Server wie den Host ausführen, führt der SnapManager-Server die Authentifizierung durch, indem Sie die Benutzernamen und Passwörter des Betriebssystems verwenden. Wenn Sie nicht zur Eingabe Ihrer OS-Passwörter aufgefordert werden möchten, können Sie die Daten unter Verwendung des Befehls smo cridential set -Host im SnapManager-Benutzeranmeldungs-Cache speichern.

Der Befehl smo Anmeldeinformation set -Host speichert Ihre Anmeldeinformationen, wenn die Eigenschaft Host.anmeldungs.persist in der Datei smo.config auf true gesetzt ist.

Beispiel

Benutzer1 und User2 teilen sich ein Profil namens Prof2. User2 kann eine Sicherung von „database1“ in Host1 nicht ohne die Berechtigung zum Zugriff auf Host1 durchführen. User1 kann eine Datenbank nicht ohne Berechtigung zum Zugriff auf host3 klonen.

In der folgenden Tabelle werden die verschiedenen Berechtigungen beschrieben, die den Benutzern zugewiesen sind:

Berechtigungstyp	Benutzer1	Benutzer2
Host-Passwort	Host1, Host2	Host2, Host3
Repository-Kennwort	Repos. 1	Repos. 1
Profilkennwort	Prof1, Prof2	Prof2

Wenn User1 und User2 keine freigegebenen Profile haben, nimmt an, dass User1 Berechtigungen für die Hosts mit Namen Host1 und Host2 hat, und User2 hat Berechtigungen für den Host namens Host2. User2 kann nicht einmal die nicht-profilbefehlen wie dump und System verify auf Host1 ausführen.

Online-Hilfe aufrufen und drucken

Die Online-Hilfe enthält Anweisungen zu den Aufgaben, die Sie über die grafische Benutzeroberfläche von SnapManager ausführen können. Die Online-Hilfe enthält auch Beschreibungen der Felder in den Fenstern und Assistenten.

1. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Hauptfenster auf **Hilfe** > **Hilfe Inhalt**.
   - Klicken Sie in einem beliebigen Fenster oder Assistenten auf **Hilfe**, um Hilfe für dieses Fenster anzuzeigen.
2. Verwenden Sie das **Inhaltsverzeichnis** im linken Fensterbereich, um durch die Themen zu navigieren.
3. Klicken Sie oben im Hilfefenster auf das Druckersymbol, um einzelne Themen zu drucken.

Überlegungen zur Implementierung von SnapManager für Oracle

Bevor Sie SnapManager in Ihrer Umgebung implementieren, sollten Sie sich mit den anderen Applikationen und Technologien vertraut machen, die für verschiedene Vorgänge erforderlich sind.

In der folgenden Tabelle sind die verschiedenen Applikationen und Technologien aufgeführt:

Anwendungen und Technologien	Details
Data ONTAP	SnapManager nutzt NetApp Tools und Technologien einschließlich Snapshot Kopien.
SnapDrive für Windows	SnapManager verwendet die Funktionen von SnapDrive. Sie müssen SnapDrive installieren, bevor Sie die SnapManager-Dienste ausführen. SnapManager übernimmt alle Interaktionen mit SnapDrive. SnapDrive für Windows muss korrekt für Ihr Storage-System und Ihre Auswahl an Protokollen konfiguriert sein.
SnapRestore	SnapManager reduziert mit SnapRestore die durchschnittliche Zeit zum Recovery einer Datenbank. Jedes Storage-System sollte über eine SnapRestore-Lizenz verfügen.
FlexClone	FlexClone ist eine lizenzierte Funktion in Data ONTAP.
FC- und iSCSI-Protokolle	Sie benötigen die lizenzierten Versionen der entsprechenden Protokolle.

Verwandte Informationen

"SnapManager for Oracle Best Practices: media.netapp.com/documents/tr-3761.pdf"

Anforderungen für die Ausführung von SnapManager

Vor dem Einsatz von SnapManager in Ihrer Umgebung sollten Sie die unterschiedlichen Anforderungen kennen.

Vor der Verwendung von SnapManager müssen Sie die Kompatibilitätsmatrizen für alle erforderlichen Produkte überprüfen. Außerdem müssen Sie Folgendes überprüfen:

- SnapManager und SnapDrive Kompatibilitätsmatrix im Abschnitt Interoperabilität finden Sie die neueste Version und Patch-Informationen für alle Hosts, Storage-Systeme und andere Komponenten, die in diesem Abschnitt aufgeführt sind.
- Konfigurationsleitfaden für NetApp FCP- und iSCSI-Produkte.

SnapManager erfordert bestimmte Oracle Versionen auf einigen Plattformen.

Weitere Informationen zu den empfohlenen Konfigurationen für Host- und Speichersysteme finden Sie im Dokumentationskit.

Wenden Sie sich an Ihren Ansprechpartner, wenn Sie eine SnapManager-Konfiguration benötigen, die nicht im Dokumentation-Kit aufgeführt ist.

Verwandte Informationen

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Unterstützte Host-Hardware

Bedenken Sie die Anforderungen an Arbeitsspeicher, Speicherplatz und CPU.

Für SnapManager ist folgende Konfiguration erforderlich:

Hardwarefunktion	Hardwareanforderungen
Speicher	Der SnapManager-Server benötigt 128 MB Arbeitsspeicher. Die grafischen Benutzeroberflächen erfordern mindestens 512 MB RAM. Jeder Vorgang, der vom SnapManager-Server ausgeführt wird, benötigt während der Ausführung 48 MB zusätzlichen Speicher.
Festplattenspeicher benötigen	128 MB verfügbarer Speicherplatz für die grafische Benutzeranwendung (Minimum).
CPU-Geschwindigkeit	1.0 GHz Prozessorgeschwindigkeit (mindestens).

Unterstützte allgemeine Konfigurationen

Vor der Installation von SnapManager müssen Sie die allgemeinen Konfigurationsanforderungen kennen.

SnapManager unterstützt folgende allgemeine Konfigurationen:

- Eine nicht-geclusterte Konfiguration, in der ein einzelner Host mit einem einzelnen Speichersystem verbunden ist
- Eine SnapManager Serverinstanz pro Host
- Jede Topologie umfasst Storage-Systeme mit Data ONTAP Controller-Failover

Informationen zu allen von SnapManager unterstützten Storage-Typen und -Versionen finden Sie in der Kompatibilitätsmatrix für SnapManager und SnapDrive.

Cluster-Konfigurationen

SnapManager arbeitet in Cluster-Konfigurationen.

SnapManager unterstützt dasselbe Host-Cluster und dieselben Konfigurationen, die das SnapDrive Produkt- und Host Utilities Kit unterstützen.

SnapManager unterstützt auch Konfigurationen ohne Cluster, bei denen ein einzelner Host mit einem einzelnen Storage-System, unterstützten Host-Clustern und Storage-Systemen verbunden ist, die einen Data ONTAP Controller Failover ausführen.

Versionsunterstützung und Übersicht über die Konfiguration der Datenbank

Sie müssen die verschiedenen Datenbankversionen und Konfigurationen kennen, die von SnapManager unterstützt werden. Sie müssen ein grundlegendes Datenbanklayout und eine grundlegende Konfiguration durchführen, um einen erfolgreichen Betrieb zu gewährleisten.

SnapManager für Oracle lässt sich mit den Versionen 10gR2 (10.2.0.5), 11gR1, 11gR2 (11.2.0.1 und 11.2.0.2) und 12__c_, mit nativer Oracle Technologie wie Recovery Manager (RMAN) sowie über Fibre Channel (FC) und iSCSI (Internet Small Computer System Interface) hinweg integrieren.

Die Oracle Database 9i wird von SnapManager 3.2 und 10g R2 (früher als 10.2.0.5) nicht unterstützt. SnapManager 3.3 wird nicht unterstützt.

Wenn Sie Oracle Datenbanken implementieren, die von SnapManager für Oracle gemanagt werden sollen, finden Sie Informationen unter „ *SnapManager for Oracle Best Practices*“.

"SnapManager for Oracle Best Practices: media.netapp.com/documents/tr-3761.pdf"

Allgemeines Layout und Konfiguration

Informationen zu den empfohlenen allgemeinen Datenbank-Layouts und Storage-Konfigurationen finden Sie, um Festplattengruppen, Dateitypen und Tablespaces zu vermeiden.

- Enthalten Sie keine Dateien aus mehr als einem SAN-Dateisystem in Ihrer Datenbank.

  Alle Dateien, die eine Datenbank erstellen, müssen sich auf demselben Dateisystem befinden.

- SnapManager erfordert mehrere 4 KB Blockgröße.
- Wenn Sie SnapManager-Backups mit dem Oracle Recovery Manager (RMAN) registrieren möchten, müssen Sie RMAN-fähige Profile erstellen.

Nachfolgend sind einige Richtlinien für die Volume-Trennung aufgeführt:

- Die Datendateien für nur eine Datenbank müssen sich im Volume befinden.
- Sie müssen separate Volumes für jede der folgenden Dateiklassifizierungen verwenden: Datenbankbinärdateien, Datendateien, Online-Wiederherstellungsprotokolle, archivierte Wiederherstellungsprotokolle und Kontrolldateien.
- Sie müssen kein separates Volume für temporäre Datenbankdateien erstellen, da SnapManager keine

temporären Datenbankdateien erstellt.

Weitere Informationen finden Sie im *SnapManager for Oracle Best Practices*.

Verwandte Informationen

"SnapManager for Oracle Best Practices: media.netapp.com/documents/tr-3761.pdf"

Beispiel für Datenbank-Volume-Layouts

Weitere Informationen zur Konfiguration Ihrer Datenbank finden Sie unter Beispiel-Datenbank-Volume-Layouts.

Single-Instance-Datenbanken

Dateitypen	Volume-Namen	Dediziertes Volume für Dateitypen	Automatische Snapshot Kopien
Oracle-Binärdateien	Orabin_Host-Name	Ja.	Ein
Datendateien	Oradata_sid	Ja.	Aus
Temporäre Datendateien	Oratep_sid	Ja.	Aus
Kontrolldateien	Oracntrl01_sid (Multiplexed) Oracntrl02_sid (Multiplexed)	Ja.	Aus
Wiederherstellungsprotokolle	Oralogen01_sid (Multiplexed) Oralogen02_sid (Multiplexed)	Ja.	Aus
Archivprotokolle	Oraarch_sid	Ja.	Aus

Einschränkungen bei der Arbeit mit SnapManager

Sie müssen die Szenarien und Einschränkungen kennen, die sich auf Ihre Umgebung auswirken können.

Einschränkungen im Zusammenhang mit Datenbank-Layouts und Plattformen

- SnapManager unterstützt Steuerdateien auf einem Dateisystem und unterstützt keine Steuerdateien auf RAW-Geräten.
- SnapManager arbeitet in einer Microsoft Clustering-Umgebung (MSCS), erkennt jedoch den Status der MSCS-Konfiguration (aktiv oder passiv) nicht und überträgt kein aktives Management eines Repositorys in einen Standby-Server in einem MSCS-Cluster.

- Die Repository-Datenbank kann auf einem Host vorhanden sein, auf den über mehrere IP-Adressen zugegriffen werden kann.

  Wenn über mehrere IP-Adressen auf das Repository zugegriffen wird, wird die Zeitplandatei für jede der IP-Adressen erstellt. Wenn die Backup-Planung für ein Profil (z. B. Profil A) unter einer der IP-Adressen (z. B. IP1) erstellt wird, wird die Zeitplandatei nur für diese IP-Adresse aktualisiert. Wenn von einer anderen IP-Adresse auf Profil A zugegriffen wird (z. B. IP2), wird das geplante Backup nicht aufgeführt, da die Terminplandatei von IP2 keinen Eintrag für den unter IP1 erstellten Zeitplan hat.

  Sie können warten, bis der Zeitplan von dieser IP-Adresse und der Zeitplandatei ausgelöst wird, oder Sie können den Server neu starten.

Einschränkungen in Bezug auf die SnapManager-Konfiguration

- SnapManager kann für die Katalogisierung von Datenbank-Backups mit RMAN konfiguriert werden.

  Wenn ein RMAN-Wiederherstellungskatalog verwendet wird, muss sich der Wiederherstellungskatalog in einer anderen Datenbank befinden als die gesicherte Datenbank.

- SnapManager unterstützt Datenbanken auf MultiStore Storage-Systemen unter folgenden Anforderungen:
  - Sie müssen SnapDrive konfigurieren, um Passwörter für MultiStore Storage-Systeme festzulegen.
  - SnapDrive kann keine Snapshot Kopie einer LUN oder Datei in einem qtree in einem MultiStore Storage-System erstellen, wenn sich das zugrunde liegende Volume nicht im selben MultiStore Storage-System befindet.
- SnapManager unterstützt nicht den Zugriff auf zwei SnapManager Server, die auf verschiedenen Ports über einen einzelnen Client laufen (sowohl über CLI als auch über GUI).

  Die Port-Nummern sollten auf dem Ziel- und den Remote-Hosts identisch sein.

- SnapManager-Vorgänge schlagen fehl und Sie können nicht auf die GUI zugreifen, wenn die Repository-Datenbank ausfällt.

  Sie müssen überprüfen, ob die Repository-Datenbank ausgeführt wird, wenn Sie SnapManager-Vorgänge durchführen.

- SnapManager unterstützt keine Live Partition Mobility (LPM) und Live Application Mobility (LAM).
- SnapManager unterstützt Oracle Wallet Manager und Transparent Data Encryption (TDE) nicht.
- MetroCluster-Konfigurationen werden von SnapManager in RDM-Umgebungen (Raw Device Mapping) nicht unterstützt, da MetroCluster-Konfigurationen noch von der Virtual Storage Console (VSC) unterstützt werden müssen.

Einschränkungen im Zusammenhang mit der Profilverwaltung

- Wenn Sie das Profil aktualisieren, um die Backups des Archivprotokolls voneinander zu trennen, können Sie auf dem Host keinen Rollback-Vorgang durchführen.
- Wenn Sie ein Profil von der GUI aktivieren, um Archiv-Protokoll-Backups zu erstellen, und später versuchen, das Profil mithilfe des Fensters „Multi Profile Update“ oder des Fensters „Profile Update“ zu aktualisieren, können Sie dieses Profil nicht ändern, um ein vollständiges Backup zu erstellen.
- Wenn Sie im Fenster Multi Profile Update mehrere Profile aktualisieren und bei einigen Profilen die Option **Backup Archivilogs separat** aktiviert ist und andere Profile die Option deaktiviert haben, ist die Option **Archivprotokolle separat** sichern deaktiviert.

- Wenn Sie mehrere Profile aktualisieren und einige Profile die Option **Backup Archivilogs separat** aktivieren und andere Profile die Option deaktiviert haben, ist die Option **Backup Archivilogs separat** im Fenster Multi Profile Update deaktiviert.
- Wenn Sie das Profil umbenennen, können Sie den Host nicht zurückführen.

Einschränkungen im Zusammenhang mit Rolling Upgrade oder Rollback-Vorgängen

- Wenn Sie versuchen, eine frühere Version von SnapManager für einen Host zu installieren, ohne den Rollback-Vorgang auf dem Host im Repository durchzuführen, können Sie Folgendes möglicherweise nicht ausführen:
  - Sehen Sie sich die Profile an, die in früheren oder neueren Versionen von SnapManager für den Host erstellt wurden.
  - Greifen Sie auf Backups oder Klone zu, die in früheren oder neueren Versionen von SnapManager erstellt wurden.
  - Führen Sie Rolling Upgrade- oder Rollback-Vorgänge auf dem Host durch.
- Nachdem Sie die Profile getrennt haben, um Backups für Archivprotokolle zu erstellen, können Sie im zugehörigen Host Repository keinen Rollback-Vorgang durchführen.

Einschränkungen im Zusammenhang mit Backup-Vorgängen

- Wenn der Backup während der Recovery bereits angehängt ist, mounted SnapManager den Backup nicht erneut und verwendet das bereits bereitgestellte Backup.

  Wenn das Backup von einem anderen Benutzer gemountet wird und Sie keinen Zugriff auf das zuvor bereitgestellte Backup haben, muss der andere Benutzer Ihnen die Berechtigung erteilen.

  Alle Archivprotokolldateien haben Leseberechtigung für Benutzer, die einer Gruppe zugewiesen sind. Sie haben möglicherweise nicht die Zugriffsberechtigung für die Archivprotokolldatei, wenn das Backup von einer anderen Benutzergruppe gemountet wird. Benutzer können die gemounteten Archivprotokolldateien manuell erteilen und den Wiederherstellungsvorgang oder die Wiederherstellung wiederholen.

- SnapManager legt den Backup-Status als „`PROTECTED`“ fest, selbst wenn eine der Snapshot-Kopien des Datenbank-Backups auf das sekundäre Storage-System übertragen wird.
- Sie können die Aufgabenspezifikationsdatei nur für geplante Backups aus SnapManager 3.2 oder höher verwenden.
- Wenn die Repository-Datenbank auf mehr als eine IP-Adresse verweist und jede IP-Adresse einen anderen Hostnamen hat, ist der Backup-Planungsvorgang für eine IP-Adresse erfolgreich, schlägt aber für die andere IP-Adresse fehl.
- In ONTAP Umgebungen unterstützt SnapManager nicht mehrere sekundäre Ziele für ein Quell-Volume.

Einschränkungen im Zusammenhang mit Wiederherstellungsvorgängen

- SnapManager unterstützt nicht die Wiederherstellung von Datenbank-Backups mithilfe eines schnellen Wiederherstellens oder von Volume-basierten Restore-Vorgängen in Windows.

  SnapManager 3.3 zeigt eine Fehlermeldung an, wenn Sie versuchen, eine schnelle Wiederherstellung aus der SnapManager CLI durchzuführen.

Einschränkungen im Zusammenhang mit Klonvorgängen

- SnapManager 3.3 oder höher unterstützt nicht mit der XML-Datei für die Klonspezifikation, die in den

Versionen vor SnapManager 3.2 erstellt wurde.

- Wenn sich temporäre Tablespaces an einem anderen Speicherort als dem Datendateien befinden, erstellt ein Klonvorgang die Tabellen im Datendateien.

  Wenn jedoch temporäre Tablespaces Oracle Managed Files (OMFs) sind, die sich an einem anderen Speicherort als dem Datendateien befinden, erstellt der Klonvorgang nicht die Tabellen im Datendateien. Die OMFs werden nicht von SnapManager verwaltet.

- SnapManager kann eine RAC Datenbank nicht klonen, wenn Sie die Option -resetlogs auswählen.

Einschränkungen im Zusammenhang mit Archiv-Log-Dateien und Backups

- SnapManager unterstützt keine Anschnitt von Archiv-Log-Dateien aus dem Flash-Recovery-Bereich Ziel.
- SnapManager unterstützt nicht das Aufheben von Archivprotokolldateien vom Standby-Ziel.
- Die Backups für das Archivprotokoll werden basierend auf der Aufbewahrungsdauer und der standardmäßigen stündlichen Aufbewahrungsklasse beibehalten.

  Wenn die Klasse für die Backup-Aufbewahrung des Archivprotokolls über die SnapManager Befehlszeilenschnittstelle oder Benutzeroberfläche geändert wird, gilt die geänderte Aufbewahrungsklasse nicht für das Backup, da die Backups des Archivprotokolls basierend auf der Aufbewahrungsdauer aufbewahrt werden.

- Wenn Sie die Archivprotokolldateien aus den Zielen des Archivprotokolls löschen, enthält die Backup des Archivprotokolls keine Archivprotokolldateien, die älter sind als die fehlende Archivprotokolldatei.

  Wenn die letzte Archivprotokolldatei fehlt, schlägt die Sicherung des Archivprotokolls fehl.

- Wenn Sie die Archivprotokolldateien aus den Archivprotokollzielen löschen, schlägt das Beschneiden von Archivprotokolldateien fehl.
- SnapManager konsolidiert die Archiv-Log-Backups, selbst wenn Sie die Archiv-Log-Dateien aus den Archiv-Log-Zielen löschen oder wenn die Archiv-Log-Dateien beschädigt sind.

Einschränkungen im Zusammenhang mit der Änderung des Host-Namens der Zieldatenbank

Die folgenden SnapManager Vorgänge werden nicht unterstützt, wenn Sie den Host-Namen der Zieldatenbank ändern:

- Ändern des Host-Namens der Zieldatenbank von der SnapManager-GUI.
- Rollback der Repository-Datenbank nach Aktualisierung des Host-Namens der Zieldatenbank des Profils durchführen.
- Gleichzeitige Aktualisierung mehrerer Profile für einen neuen Hostnamen der Zieldatenbank.
- Ändern des Host-Namens der Zieldatenbank, wenn ein SnapManager-Vorgang ausgeführt wird.

Einschränkungen im Zusammenhang mit der SnapManager CLI oder GUI

- Die CLI-Befehle von SnapManager für den Vorgang zum Erstellen von Profilen, die über die Benutzeroberfläche von SnapManager generiert werden, verfügen über keine Optionen zur Verlaufskonfiguration.

  Mit dem Befehl „Profile create“ können Sie die Verlaufs-Aufbewahrungseinstellungen über die SnapManager-CLI konfigurieren.

- SnapManager zeigt die GUI in Mozilla Firefox nicht an, wenn auf dem Windows-Client keine Java Runtime Environment (JRE) verfügbar ist.
- SnapManager 3.3 zeigt die SnapManager-Benutzeroberfläche in Microsoft Internet Explorer 6 unter Windows Server 2008 und Windows 7 nicht an.
- Wenn beim Aktualisieren des Host-Namens der Zieldatenbank mithilfe der SnapManager CLI eine oder mehrere offene SnapManager GUI-Sitzungen vorliegen, reagieren nicht alle offenen SnapManager GUI-Sitzungen.
- Wenn Sie SnapManager unter Windows installieren und die CLI in UNIX starten, werden die Funktionen angezeigt, die unter Windows nicht unterstützt werden.

Einschränkungen im Zusammenhang mit SnapMirror und SnapVault

- In einigen Szenarien können Sie das letzte Backup, das mit der ersten Snapshot Kopie verbunden ist, nicht löschen, wenn das Volume eine SnapVault-Beziehung eingerichtet hat.

  Sie können das Backup nur löschen, wenn Sie die Beziehung unterbrechen. Dieses Problem liegt an einer ONTAP-Einschränkung bei Basis-Snapshot-Kopien. In einer SnapMirror Beziehung wird die Snapshot Basiskopie von der SnapMirror Engine erstellt und in einer SnapVault Beziehung ist die Snapshot Basiskopie das Backup, das mit SnapManager erstellt wurde. Die Basis-Snapshot-Kopie verweist bei jedem Update auf das neueste Backup, das mithilfe von SnapManager erstellt wird.

Einschränkungen im Zusammenhang mit Data Guard Standby-Datenbanken

- SnapManager unterstützt keine Standby-Datenbanken für die logische Datenwache.
- SnapManager unterstützt keine Standby-Datenbanken für Active Data Guard.
- SnapManager erlaubt keine Online-Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine partiellen Backups von Data Guard Standby-Datenbanken.
- SnapManager erlaubt nicht die Wiederherstellung von Data Guard Standby-Datenbanken.
- SnapManager erlaubt keine Beschneidung von Archivprotokolldateien für Data Guard Standby-Datenbanken.
- SnapManager unterstützt den Broker nicht.

Verwandte Informationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

SnapManager Funktionen und Oracle Technologien, die unter Windows nicht unterstützt werden

SnapManager unterstützt einige SnapManager Funktionen, Plattformen und Oracle-Technologien nicht unter Windows.

SnapManager bietet keine Unterstützung für folgende Funktionen, Plattformen und Oracle Technologien:

- Richtlinienbasierte Datensicherung mit der Integration von Protection Manager
- Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) im Operations Manager verfügbar
- Schnelle Wiederherstellung oder Volume-basierte SnapRestore (VBSR)
- Klonteilvorgang

- Oracle Real Application Clusters (RAC) mit jedem beliebigen Protokoll
- Oracle Automatic Storage Management (ASM) mit einem beliebigen Protokoll
- Oracle Direct NFS (dNFS)
- Itanium-64-Plattformen

Die unterstützten Hardwareplattformen für das Windows-Betriebssystem sind 32-Bit und 64-Bit (Windows x86 und Windows x86_64).

SnapManager Limitierungen für Clustered Data ONTAP

Sie müssen die Einschränkungen für einige Funktionalitäten und SnapManager-Vorgänge kennen, wenn Sie Clustered Data ONTAP verwenden.

Die folgenden Funktionalitäten werden nicht unterstützt, wenn Sie SnapManager auf Clustered Data ONTAP nutzen:

- RDM (Raw Device Mapping) Logical Unit Number (LUN) für Storage Virtual Machines (SVM)
- Eine Datenbank, in der eine LUN zu einem System gehört, auf dem Data ONTAP 7-Mode und die andere LUN ausgeführt werden, gehört zu einem System mit Clustered Data ONTAP
- SnapManager für Oracle unterstützt keine Migration von Vserver, wie sie von Clustered Data ONTAP nicht unterstützt wird
- SnapManager für Oracle unterstützt die Funktion Clustered Data ONTAP 8.2.1 nicht zur Festlegung verschiedener Exportrichtlinien für Volumes und qtrees

Einschränkungen in Bezug auf Oracle Database

Bevor Sie mit der Arbeit mit SnapManager beginnen, müssen Sie die Einschränkungen in Bezug auf Oracle Database kennen.

Die Einschränkungen sind wie folgt:

- SnapManager unterstützt Oracle Versionen 10gR2, 11gR1, 11gR2 und 12*c*, unterstützt aber Oracle 10gR1 als Repository oder Zieldatenbank nicht.
- SnapManager unterstützt die Verwendung einer SCAN-IP-Adresse anstelle eines Hostnamens nicht.

  SCAN-IP ist eine neue Funktion in Oracle 11gR2.

- Oracle Cluster File System (OCFS) wird von SnapManager nicht unterstützt.
- Unterstützung für Oracle Database 9i ist veraltet aus SnapManager 3.2.
- Der Support für Oracle Database 10gR2 (früher als 10.2.0.5) ist veraltet aus SnapManager 3.3.1.

Ermitteln Sie die verschiedenen Versionen von Oracle Datenbanken, die durch die Interoperabilitäts-Matrix unterstützt werden.

Verwandte Informationen

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Veraltete Versionen der Oracle-Datenbank

Oracle Database 9i wird von SnapManager 3.2 oder höher nicht unterstützt, und die Oracle Database 10gR2 (früher als 10.2.0.4) wird von SnapManager 3.3.1 oder höher nicht unterstützt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und auf SnapManager 3.2 oder höher aktualisieren möchten, können Sie keine neuen Profile erstellen. Eine Warnmeldung wird angezeigt.

Wenn Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken verwenden und ein Upgrade auf SnapManager 3.2 oder höher durchführen möchten, müssen Sie eine der folgenden Aktionen durchführen:

- Aktualisieren Sie Oracle 9i oder 10gR2 (früher als 10.2.0.4) Datenbanken auf entweder Oracle 10gR2 (10.2.0.5), 11gR1 oder 11gR2 Datenbanken und führen Sie ein Upgrade auf SnapManager 3.2 oder 3.3 durch.

  Wenn Sie ein Upgrade auf Oracle 12*c* durchführen, müssen Sie ein Upgrade auf SnapManager 3.3.1 oder höher durchführen.

  Oracle Datenbank 12*c* wird nur von SnapManager 3.3 unterstützt.

- Verwalten Sie die Oracle 9i-Datenbanken mit einer Patch-Version von SnapManager 3.1.

  Sie können SnapManager 3.2 oder 3.3 verwenden, wenn Sie Oracle 10gR2-, 11gR1- oder 11gR2-Datenbanken verwalten und SnapManager 3.3.1 oder höher verwenden möchten, wenn Sie Oracle 12*c* -Datenbanken zusammen mit anderen unterstützten Datenbanken verwalten möchten.

Installation von SnapManager für Oracle

Sie können SnapManager für Oracle in Ihre Umgebung herunterladen und installieren, beispielsweise um Vorgänge wie Datenbank-Backup, -Wiederherstellung, -Recovery und -Klonen auszuführen.

Das Installationspaket SnapManager für Oracle enthält die Host Server Software und die Client-Software der grafischen Benutzeroberfläche (GUI).

Installation von SnapManager für Oracle wird vorbereitet

Die Umgebung, in der Sie SnapManager für Oracle installieren, muss bestimmte Software-, Hardware-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Aktuelle Informationen zu den Anforderungen finden Sie in der Interoperabilitäts-Matrix.

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Aufgaben vor der Installation

Vor der Installation von SnapManager für Oracle müssen Sie einige zusätzliche Aufgaben durchführen, um Ihre Umgebung einzurichten. Die Aufgaben, die Sie durchführen müssen, hängen vom Betriebssystem, den Oracle-Komponenten und der gewünschten Datenbankversion ab.

- Installieren Sie das lizenzierte Betriebssystem mit den entsprechenden Patches.
- Legen Sie die Sprachen des Betriebssystems und der Oracle-Datenbank auf Englisch fest.

  Um beispielsweise die Sprache der Oracle-Datenbank auf Englisch einzustellen, weisen Sie NLS_LANG = AMERICAN_AMERICA.WE8MSWIN1252 zu. Weitere Informationen zum Festlegen der Sprache finden Sie im Abschnitt „ *Troubleshooting SnapManager for Oracle*“.

- Installieren Sie den Oracle Recovery Manager (RMAN), wenn Sie RMAN mit SnapManager für Oracle verwenden möchten.
- Installieren Sie Data ONTAP mit aktivierten Lizenzen für SnapRestore und den unterstützten Protokollen wie Fibre Channel (FC) und Internet Small Computer System Interface (iSCSI) auf allen Storage-Systemen.
- Installieren Sie die folgenden Oracle Patches, wenn Sie Oracle Databases 11.2.0.2 und 11.2.0.3 verwenden:
  - 13413167 für Windows 32-Bit
  - 13555974 für Windows 64-Bit

Verwandte Informationen

SnapManager zur Fehlerbehebung

"NetApp Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

"SnapManager for Oracle Best Practices: media.netapp.com/documents/tr-3761.pdf"

Laden des Installationspakets von SnapManager für Oracle herunter

Das Installationspaket für SnapManager für Oracle kann von der NetApp Support Website heruntergeladen werden.

1. Loggen Sie sich auf der NetApp Support Site ein.
2. Klicken Sie auf der NetApp Support-Webseite auf **Downloads** > **Software**.
3. Gehen Sie in der Software-Download-Tabelle in die SnapManager-Produktzeile und wählen Sie in der Dropdown-Liste Plattform auswählen * Oracle (Windows)* aus.
4. Klicken Sie Auf **Go**.

   Die SnapManager Versionen sind aufgeführt.

5. Klicken Sie auf **Anzeigen & Herunterladen** für die SnapManager-Version, die Sie installieren möchten.

   Die Beschreibungsseite wird angezeigt.

   Sie sollten die auf dieser Seite verfügbaren Informationen lesen.

6. Klicken Sie unten auf dieser Seite auf **Weiter**.

   Die Seite Lizenzvertrag wird angezeigt.

   Sie sollten die auf dieser Seite verfügbaren Informationen lesen.

7. Klicken Sie Auf **Akzeptieren**.

   Die Download-Seite wird angezeigt.

8. Laden Sie das Installationspaket für Ihren Host herunter.

   Sie können die Installationsdatei an einen beliebigen Speicherort auf dem Computer herunterladen, auf dem Sie SnapManager für Oracle installieren möchten.

"NetApp Support Website: mysupport.netapp.com"

Installation von SnapManager für Oracle

Sie können SnapManager auf dem Host installieren, der über eine oder mehrere Datenbanken zu managen ist. Sie können nur eine SnapManager-Instanz pro Host installieren.

- Sie müssen die erforderlichen Vorinstallationsaufgaben abgeschlossen haben.
- Das neueste SnapManager Installationspaket muss heruntergeladen werden.
- Die entsprechende Version von SnapDrive für Windows muss auf allen Ziel-Hosts installiert und konfiguriert sein.

  Informationen zum Installieren und Konfigurieren von SnapDrive für Windows finden Sie unter *SnapDrive for Windows Installation and Administration Guide*.

  a. Doppelklicken Sie auf die SnapManager-Installationsdatei:

Wenn das Betriebssystem…	Verwenden Sie dann…
Windows x86	netapp.smo.windows-x86-version.exe
Windows x64	netapp.smo.windows-x64-version.exe

  Die folgende Meldung wird angezeigt: Der Herausgeber konnte nicht überprüft werden. Möchten Sie diese Software wirklich ausführen?

  b. Klicken Sie auf **OK**.

  c. Klicken Sie im Fenster Einführung auf **Weiter**.

  d. Klicken Sie im Fenster Installationsordner auswählen entweder auf **Weiter**, um den Standardinstallationsspeicher zu akzeptieren, oder wählen Sie einen neuen Speicherort aus.

  Der Standardspeicherort ist: C:\Programme\NetApp\SnapManager für Oracle.

  e. Klicken Sie im Fenster Menüverfügbarkeit auf **Weiter**.

  f. Geben Sie im Fenster Diensteigenschaften angeben die Konto- und Kennwortinformationen für den Windows-Dienst ein.

  Das angegebene Konto muss Mitglied der folgenden Gruppen sein:

  - Die lokale Administrationsgruppe des Speichersystems

- Die lokale Administratorgruppe
- Die ORA_DBA-Gruppe, die Sie angeben können, ob der Dienst nach einem Neustart automatisch gestartet werden muss oder manuell gestartet werden soll.

g. Klicken Sie im Fenster Übersicht vor der Installation auf **Installieren**.

h. Klicken Sie im Fenster „Installation abgeschlossen“ auf **Weiter**.

i. Klicken Sie im Fenster wichtige Informationen auf **Fertig**, um den Installer zu beenden.

Nach Abschluss der Installation können Sie überprüfen, ob die Installation erfolgreich war:

1. Starten Sie den SnapManager-Server:
   a. Wählen Sie im Fenster Windows-Dienste **NetApp-SnapManager-Version für Oracle** aus.
   b. Klicken Sie im linken Bereich auf **Start**.
2. Vergewissern Sie sich, dass das SnapManager System ordnungsgemäß ausgeführt wird:
   a. Klicken Sie auf **Start** > **Programme** > **NetApp** > **SnapManager für Oracle** > **Start SMO Command Line Interface (CLI)**.
   b. Geben Sie in der Befehlszeilenschnittstelle (CLI) den folgenden Befehl ein: smo System überprüfen Sie, ob die folgende Meldung angezeigt wird: Operation ID number sukzceded.

   Nummer ist die Vorgangs-ID-Nummer.

Verwandte Informationen

Installation von SnapManager für Oracle wird vorbereitet

Aufgaben vor der Installation

Laden des Installationspakets von SnapManager für Oracle herunter

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Upgrade von SnapManager

Sie können von einer der früheren Versionen auf die neueste Version von SnapManager für Oracle aktualisieren. Sie können entweder alle SnapManager Hosts gleichzeitig aktualisieren oder ein Rolling Upgrade durchführen, wodurch Sie die Hosts auf gestaffelte, Host-für-Host-Art aktualisieren können.

SnapManager wird vorbereitet

Die Umgebung, in der Sie ein SnapManager-Upgrade durchführen möchten, muss die spezifischen Software-, Hardware-, Browser-, Datenbank- und Betriebssystemanforderungen erfüllen. Aktuelle Informationen zu den Anforderungen finden Sie in der Interoperabilitäts-Matrix.

Sie müssen vor dem Upgrade sicherstellen, dass Sie die folgenden Aufgaben ausführen:

- Führen Sie die erforderlichen Vorinstallationsaufgaben aus.

- Laden Sie das neueste Installationspaket von SnapManager für Oracle herunter.
- Installieren und konfigurieren Sie die entsprechende Version von SnapDrive für Windows auf allen Ziel-Hosts.
- Erstellen eines Backups der vorhandenen Repository-Datenbank SnapManager für Oracle

"Interoperabilitäts-Matrix: support.netapp.com/NOW/products/interoperability"

Aktualisieren von SnapManager-Hosts

Sie können ein Upgrade aller vorhandenen SnapManager-Hosts durchführen, um die neueste Version von SnapManager zu verwenden. Alle Hosts werden gleichzeitig aktualisiert. Dies kann jedoch zu einer Ausfallzeit aller SnapManager-Hosts und der geplanten Operationen während dieser Zeit führen.

1. Stoppen Sie den SnapManager-Server, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie im Fenster Windows-Dienste **NetApp SnapManager für Oracle** aus.
   b. Klicken Sie im linken Bereich auf **Stopp**.
2. Doppelklicken Sie auf die SnapManager-Installationsdatei.

Wenn das Betriebssystem…	Verwenden Sie dann…
Windows x86	netapp.smo.windows-x86-version_number.exe
Windows x64	netapp.smo.windows-x64-version_number.exe

   Die folgende Meldung wird angezeigt: Der Herausgeber konnte nicht überprüft werden. Möchten Sie diese Software wirklich ausführen?

3. Klicken Sie auf **OK**.

   Das Fenster Einführung wird angezeigt.

4. Klicken Sie Auf **Weiter**.

   Das Fenster Installationsordner auswählen wird angezeigt.

5. Klicken Sie auf **Weiter**, um den Standard-Installationsort zu akzeptieren oder einen neuen Speicherort auszuwählen.

   Der Standardspeicherort ist: C:\Programme\NetApp\SnapManager für Oracle.

6. Klicken Sie im Fenster Menüverfügbarkeit auf **Weiter**.
7. Geben Sie im Fenster Diensteigenschaften angeben die Konto- und Kennwortinformationen für den Windows-Dienst ein.

   Das angegebene Konto muss Mitglied der folgenden Gruppen sein:

   - Die lokale Administrationsgruppe des Speichersystems
   - Die lokale Administratorgruppe

◦ Die ORA_DBA-Gruppe, die Sie angeben können, ob der Dienst nach dem Neustart automatisch gestartet werden muss oder der Dienst manuell gestartet werden muss.

8. Klicken Sie im Fenster Übersicht vor der Installation auf **Installieren**.
9. Klicken Sie im Fenster „Installation abgeschlossen“ auf **Weiter**.
10. Klicken Sie im Fenster wichtige Informationen auf **Fertig**, um den Installer zu beenden.

Verwandte Informationen

Installation von SnapManager für Oracle wird vorbereitet

Aufgaben vor der Installation

Laden des Installationspakets von SnapManager für Oracle herunter

Aufgaben nach dem Upgrade

Nach dem Upgrade auf eine neuere Version von SnapManager müssen Sie das vorhandene Repository aktualisieren. Sie können auch die Backup-Aufbewahrungsklasse ändern, die den vorhandenen Backups zugewiesen ist.

Nach dem Upgrade auf SnapManager 3.3 oder höher müssen Sie sqlnet.authentication_services auf NONE setzen, wenn Sie die Datenbank-Authentifizierung (DB) als einzige Authentifizierungsmethode verwenden möchten. Diese Funktion wird für RAC-Datenbanken nicht unterstützt.

Das vorhandene Repository wird aktualisiert

Sie müssen das vorhandene Repository nicht aktualisieren, wenn Sie ein Upgrade von SnapManager 3.3.x auf SnapManager 3.4 oder höher durchführen. Für alle anderen Upgrade-Pfade müssen Sie jedoch das vorhandene Repository aktualisieren, damit Sie nach dem Upgrade darauf zugreifen können.

- Der aktualisierte SnapManager-Server muss gestartet und verifiziert worden sein.
- Ein Backup des vorhandenen Repositorys muss vorhanden sein.
- Wenn Sie ein Upgrade von einer älteren Version als SnapManager 3.1 auf SnapManager 3.3 oder höher durchführen, müssen Sie zuerst auf SnapManager 3.2 aktualisieren.

  Nach dem Upgrade auf SnapManager 3.2 können Sie dann ein Upgrade auf SnapManager 3.3 oder höher durchführen.

- Nach dem Aktualisieren des Repositorys können Sie das Repository nicht mit einer früheren SnapManager-Version verwenden.

  a. Aktualisieren Sie das vorhandene Repository: smo Repository Update -Repository -dbname Repository_Service_Name -Host Repository_Host_Name -Login -username Repository_Name -Port Repository_Port

     ▪ Der Repository-Benutzername, der Repository-Dienstname und der Repository-Hostname können aus alphanumerischen Zeichen, einem Minuszeichen, einem Unterstrich und einem Zeitraum bestehen.

- Der Repository-Port kann eine beliebige gültige Portnummer sein. Die anderen Optionen, die beim Aktualisieren des vorhandenen Repositorys verwendet werden, sind wie folgt:
- Die Option Kraft
- Die Option noprompt
- Die ruhige Option
- Die ausführliche Option

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521

+
```

Starten Sie den SnapManager-Server neu, um die zugehörigen Zeitpläne neu zu starten.

Ändern der Backup-Aufbewahrungsklasse

Der aktualisierte SnapManager weist den vorhandenen Backups die standardmäßige Backup-Aufbewahrungsklasse zu. Sie können die Standardwerte für die Aufbewahrungsklassen entsprechend Ihren Backup-Anforderungen ändern.

Die standardmäßige Backup-Aufbewahrungsklasse, die den vorhandenen Backups zugewiesen ist, lautet wie folgt:

Backup-Typ	Zuweisung von Aufbewahrungsklassen nach Upgrade
Backups werden für immer aufbewahrt	Unbegrenzt
Andere Backups	Täglich

Hinweis: Sie können die Backups löschen, die für immer aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Wenn Sie ein Upgrade auf SnapManager 3.0 oder höher durchführen, werden den vorhandenen Profilen der größere der folgenden beiden Werte zugewiesen:

- Vorherige Aufbewahrungsanzahl für das Profil
- Standardwerte für die Aufbewahrungsanzahl und die Dauer der täglichen Backups, wie in der smo.config Datei angegeben
  a. Ändern Sie die Werte, die in der Datei smo.config der Datei contac.hourly.count zugewiesen wurden, und behalten Sie.hourly.duration bei.

     Sie können die folgenden Werte eingeben:

     - Beibehalten.hourly.count = 12
     - Beibehalten.hourly.duration = 2

Verwandte Informationen

Aktualisieren von SnapManager-Hosts mithilfe von Rolling Upgrade

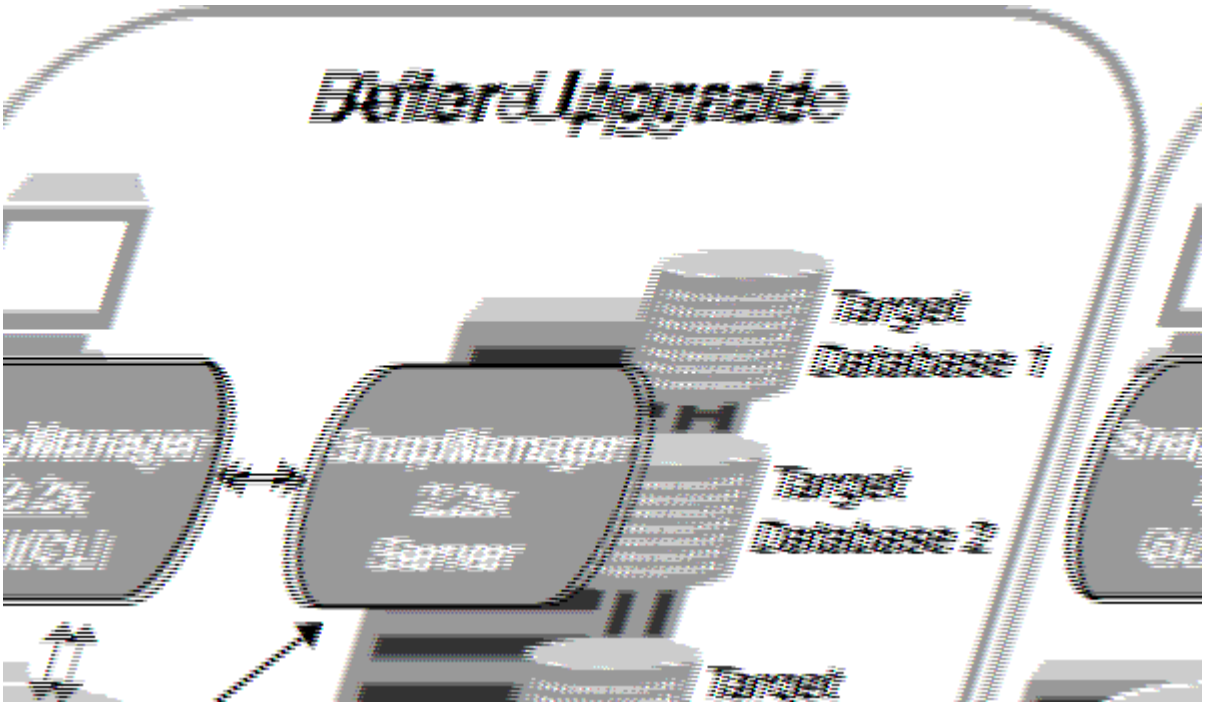
Der Rolling Upgrade-Ansatz, mit dem Sie Hosts auf gestaffelte, Host-für-Host-Art aktualisieren können, wird von SnapManager 3.1 unterstützt.

Mit SnapManager 3.0 oder einer älteren Version konnten Sie nur alle Hosts gleichzeitig aktualisieren. Dies führte zu Ausfallzeiten aller SnapManager-Hosts und der geplanten Betrieb während des Upgrade-Vorgangs.

Das Rolling Upgrade bietet folgende Vorteile:

- Verbesserte SnapManager Performance, da nur ein Host gleichzeitig aktualisiert wird.
- Fähigkeit, die neuen Funktionen auf einem SnapManager Server Host zu testen, bevor ein Upgrade der anderen Hosts durchgeführt wird

Rolling Upgrades können nur über die Befehlszeilenschnittstelle (CLI) durchgeführt werden.



Nach erfolgreichem Abschluss des Rolling Upgrade verfügen die SnapManager Hosts, Profile, Zeitpläne, Backups, Klone, die mit den Profilen der Zieldatenbanken verbunden sind, werden von der Repository-Datenbank der früheren SnapManager Version in die Repository-Datenbank der neuen Version migriert. Details zu den Vorgängen, die mithilfe der Profile, Zeitpläne, Backups und Klone, die in der früheren SnapManager Version erstellt wurden, stehen nun in der Repository-Datenbank der neuen Version zur Verfügung. Sie können die GUI mit den Standardkonfigurationswerten der Datei user.config starten. Die in der Datei User.config der früheren Version von SnapManager konfigurierten Werte werden nicht berücksichtigt.

Der aktualisierte SnapManager-Server kann jetzt mit der aktualisierten Repository-Datenbank kommunizieren. Die Hosts, die kein Upgrade durchgeführt haben, können ihre Zieldatenbanken mithilfe des Repositorys der früheren Version von SnapManager managen. Somit können die in der früheren Version verfügbaren Funktionen genutzt werden.

Bevor Sie ein Rolling Upgrade durchführen, müssen Sie sicherstellen, dass alle Hosts unter der Repository-Datenbank aufgelöst werden können. Informationen zur Lösung der Hosts finden Sie im Abschnitt zur Fehlerbehebung in *SnapManager for Oracle Administration Guide for UNIX*.

Verwandte Informationen

Was ist ein Rollback

SnapManager zur Fehlerbehebung

Voraussetzungen für das Durchführen eines Rolling Upgrades

Vor der Durchführung des Rolling Upgrades müssen Sie sicherstellen, dass Ihre Umgebung bestimmte Anforderungen erfüllt.

- Wenn Sie eine ältere Version als SnapManager 3.1 verwenden und ein Rolling Upgrade auf SnapManager 3.3 oder höher durchführen möchten, müssen Sie zuerst auf 3.2 und dann auf die neueste Version aktualisieren.

  Sie können direkt von SnapManager 3.2 auf SnapManager 3.3 oder höher aktualisieren.

- Externe Skripte, die zur Durchführung externer Datensicherung oder Datenaufbewahrung verwendet werden, müssen gesichert werden.
- Die SnapManager-Version, auf die Sie aktualisieren möchten, muss installiert sein.

  Wenn Sie ein Upgrade von einer älteren Version als SnapManager 3.1 auf SnapManager 3.3 oder höher durchführen, müssen Sie zuerst SnapManager 3.2 installieren und ein Rolling Upgrade durchführen. Nach dem Upgrade auf 3.2 können Sie SnapManager 3.3 oder höher installieren und ein weiteres Rolling Upgrade auf SnapManager 3.3 oder höher durchführen.

- Die SnapDrive für Windows-Version, die von der SnapManager-Version unterstützt wird, auf die Sie aktualisieren möchten, muss installiert sein.

  Informationen zum Installieren von SnapDrive finden Sie unter SnapDrive-Dokumentationssatz.

- Die Repository-Datenbank muss gesichert werden.
- Die SnapManager Repository-Auslastung sollte mindestens betragen.
- Wenn der zu aktualisierenden Host ein Repository verwendet, dürfen SnapManager-Vorgänge nicht auf den anderen Hosts ausgeführt werden, die dasselbe Repository verwenden.

  Die Vorgänge, die auf den anderen Hosts geplant oder ausgeführt werden, warten darauf, bis das Rolling Upgrade abgeschlossen ist.

- Profile, die auf dieselbe Repository-Datenbank verweisen, müssen mit unterschiedlichen Namen in den SnapManager-Server-Hosts erstellt werden.

  Wenn Sie Profile mit dem gleichen Namen verwenden, schlägt das Rolling Upgrade der Repository-Datenbank ohne Warnung fehl.

- SnapManager-Vorgänge dürfen nicht auf dem Host ausgeführt werden, der gerade aktualisiert wird.

Das Rolling Upgrade wird länger ausgeführt, wenn die Anzahl der Backups der Hosts, die zusammen aktualisiert werden, steigt. Die Dauer des Upgrades kann je nach Anzahl der Profile und Backups variieren, die mit einem bestimmten Host verbunden sind.

Verwandte Informationen

Installation von SnapManager für Oracle

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Durchführung von Rolling Upgrade auf einem einzelnen oder mehreren Hosts

Sie können Rolling Upgrades für einen einzelnen oder mehrere SnapManager Server Hosts über die Befehlszeilenschnittstelle (CLI) durchführen. Der aktualisierte SnapManager-Server-Host wird dann nur mit der späteren Version von SnapManager verwaltet.

Sie müssen sicherstellen, dass alle Voraussetzungen für das Durchführen eines Rolling Upgrades abgeschlossen sind.

1. Um ein Rolling Upgrade auf einem einzelnen Host durchzuführen, geben Sie den folgenden Befehl ein: Smarorepository rollingUpgrade-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-Upgradehosthost_with_target_Database-Force [-quiet

   Der folgende Befehl führt das Rolling Upgrade aller auf HostA eingebundenen Zieldatenbanken und einer Repository-Datenbank namens repoA auf repo_Host durch:

   ```
   smo repository rollingupgrade
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -upgradehost hostA
   ```

2. Um ein Rolling Upgrade auf mehreren Hosts durchzuführen, geben Sie den folgenden Befehl ein: Smarorpository rollingUpgrade-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-Upgradehosthost_with_Target_database1,Host_with_Target_database2-Force [-quiet_inverbose]

   Geben Sie bei mehreren Hosts die durch Komma getrennten Hostnamen ein, und stellen Sie sicher, dass Sie keinen Speicherplatz zwischen dem Komma und dem nächsten Hostnamen angeben.Stellen Sie außerdem sicher, dass Sie alle Hostnamen in doppelte Anführungszeichen eingeben.

   Der folgende Befehl führt das Rolling Upgrade aller auf den Hosts eingebundenen Zieldatenbanken, hostA und hostB sowie einer Repository-Datenbank namens repoA auf repo_Host durch:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -upgradehost hostA,hostB
```

3. Um ein Rolling Upgrade auf allen Hosts einer Repository-Datenbank durchzuführen, geben Sie den folgenden Befehl ein: Smorepository rollingUpgrade-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-allhosts-Force [-quiet

   Nachdem Sie die Repository-Datenbank erfolgreich aktualisiert haben, können Sie alle SnapManager-Vorgänge auf der Zieldatenbank ausführen.

   Beim aktualisierten SnapManager für Oracle bleiben die hostbasierten Benutzeranmeldeinformationen, die Anmeldedaten für Oracle Software-Benutzer und die Anmeldedaten für den Oracle Recovery Manager (RMAN) von der früheren Version von SnapManager für Oracle erhalten.

   Der folgende Befehl führt das Rolling Upgrade aller Zieldatenbanken durch, die in einer Repository-Datenbank mit dem Namen „repoA“ auf repo_Host verfügbar sind:

```
smo repository rollingupgrade
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
      -allhosts
```

   - Wenn der SnapManager-Server automatisch startet, müssen Sie den Server neu starten, um sicherzustellen, dass Sie die Zeitpläne anzeigen können.
   - Wenn Sie einen der beiden zugehörigen Hosts aktualisieren, müssen Sie nach dem ersten Upgrade des zweiten Hosts ein Upgrade durchführen.

     Wenn Sie beispielsweise einen Klon von Host A nach Host B erstellt oder ein Backup von Host A an Host B angehängt haben, hängen die Hosts A und B miteinander zusammen. Wenn Sie Host A aktualisieren, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, den Host B bald nach dem Upgrade von Host A zu aktualisieren

     Die Warnmeldungen werden angezeigt, obwohl der Klon gelöscht wurde oder das Backup während des Rolling Upgrades von Host A von Host B abgehängt wurde Dies liegt daran, dass Metadaten im Repository für die Vorgänge vorhanden sind, die auf dem Remote-Host durchgeführt werden.

Verwandte Informationen

Voraussetzungen für das Durchführen eines Rolling Upgrades

Was ist ein Rollback

Mit dem Rollback-Vorgang können Sie nach einem Rolling Upgrade auf eine frühere SnapManager-Version zurücksetzen.

Bevor Sie ein Rollback durchführen können, müssen Sie sicherstellen, dass alle Hosts unter der Repository-Datenbank aufgelöst werden können.

Wenn Sie ein Rollback durchführen, werden die folgenden Schritte zurückgesetzt:

- Backups, die erstellt, freigegeben und gelöscht wurden, verwenden Sie dazu die SnapManager Version, von der Sie ein Rollback durchführen
- Klone, die anhand eines Backups erstellt wurden, die mit der SnapManager Version erstellt wurden, von der aus Sie ein Rollback durchführen
- Profildaten wurden mithilfe der SnapManager-Version geändert, von der aus Sie ein Rollback ausführen

Die Funktionen, die in der von Ihnen verwendeten SnapManager-Version verfügbar waren, aber in der Version, auf die Sie zurückrollt, nicht verfügbar sind, werden nicht unterstützt. Wenn Sie beispielsweise ein Rollback von SnapManager 3.3 oder neuer zu SnapManager 3.1 durchführen, wird die Verlaufskonfiguration für Profile in SnapManager 3.3 oder höher nicht auf die Profile in SnapManager 3.1 zurückgesetzt. Dies liegt daran, dass die Verlaufskonfiguration in SnapManager 3.1 nicht verfügbar war.

Verwandte Informationen

SnapManager zur Fehlerbehebung

Einschränkungen bei der Durchführung eines Rollbacks

Sie müssen die Szenarien kennen, in denen Sie kein Rollback durchführen können. In einigen dieser Szenarien können Sie jedoch einige zusätzliche Aufgaben ausführen, bevor Sie das Rollback durchführen.

Die Szenarien, in denen Sie kein Rollback durchführen können oder die zusätzlichen Aufgaben ausführen müssen, sind wie folgt:

- Wenn Sie nach einem Rolling Upgrade einen der folgenden Vorgänge ausführen:
  - Erstellen Sie ein neues Profil.
  - Ändern Sie den Mount-Status des Backups.

    In diesem Szenario müssen Sie zuerst den Mount-Status in den ursprünglichen Zustand ändern und dann ein Rollback durchführen.

  - Stellen Sie ein Backup wieder her.
  - Ändern Sie den Authentifizierungsmodus von der Datenbankauthentifizierung in die Betriebssystemauthentifizierung.

    In diesem Szenario müssen Sie nach einem Rollback den Authentifizierungsmodus manuell von OS in

die Datenbank ändern.

- Wenn der Hostname des Profils geändert wird
- Wenn Profile getrennt sind, um Archiv-Log-Backups zu erstellen

  In diesem Szenario können Sie keine Rollbacks auf eine Version durchführen, die früher als SnapManager 3.2 ist.

Voraussetzungen für die Durchführung eines Rollbacks

Bevor Sie ein Rollback durchführen, müssen Sie sicherstellen, dass Ihre Umgebung bestimmte Anforderungen erfüllt.

- Wenn Sie SnapManager 3.3 oder höher verwenden und zu einer älteren Version als SnapManager 3.1 zurückkehren möchten, müssen Sie ein Rollback auf 3.2 und dann auf die gewünschte Version durchführen.
- Externe Skripte, die zur Durchführung externer Datensicherung oder Datenaufbewahrung verwendet werden, müssen gesichert werden.
- Die SnapManager-Version, auf die Sie einen Rollback ausführen möchten, muss installiert sein.

  Wenn Sie ein Rollback von SnapManager 3.3 oder neuer auf eine Version vor SnapManager 3.1 durchführen möchten, müssen Sie zuerst SnapManager 3.2 installieren und ein Rollback durchführen. Nach einem Rollback auf 3.2 können Sie SnapManager 3.1 oder eine frühere Version installieren und ein weiteres Rollback auf diese Version durchführen.

- Die SnapDrive für Windows-Version, die mit der SnapManager-Version unterstützt wird, zu der Sie einen Rollback ausführen möchten, muss installiert sein.

  Informationen zum Installieren von SnapDrive finden Sie unter SnapDrive-Dokumentationssatz.

- Die Repository-Datenbank muss gesichert werden.
- Wenn der zurückzugerollte Host ein Repository verwendet, dürfen SnapManager-Vorgänge nicht auf den anderen Hosts ausgeführt werden, die dasselbe Repository verwenden.

  Der geplante oder auf den anderen Hosts ausgeführte Betrieb wartet auf den Abschluss des Rollbacks.

- Profile, die auf dieselbe Repository-Datenbank verweisen, müssen mit unterschiedlichen Namen in den SnapManager-Server-Hosts erstellt werden.

  Wenn Sie Profile mit demselben Namen verwenden, schlägt der Rollback-Vorgang mit dieser Repository-Datenbank ohne Warnung fehl.

- SnapManager-Vorgänge dürfen nicht auf dem Host ausgeführt werden, den Sie zurücksetzen möchten.

  Wenn ein Vorgang ausgeführt wird, müssen Sie warten, bis dieser Vorgang abgeschlossen ist, und bevor Sie mit dem Rollback fortfahren.

Der Rollback-Vorgang wird längere Zeit ausgeführt, da sich die kumulative Anzahl von Backups der Hosts, die gemeinsam wieder erstellt werden, erhöht. Die Dauer des Rollbacks kann je nach Anzahl der Profile und Backups, die mit einem bestimmten Host verbunden sind, variieren.

Verwandte Informationen

Installation von SnapManager für Oracle

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Durchführen eines Rollbacks auf einem oder mehreren Hosts

Sie können auf einem oder mehreren SnapManager Server Hosts ein Rollback durchführen, indem Sie die Befehlszeilenschnittstelle (CLI) verwenden.

Sie müssen sicherstellen, dass alle Voraussetzungen für die Durchführung eines Rollbacks abgeschlossen sind.

1. Um ein Rollback auf einem einzelnen Host durchzuführen, geben Sie den folgenden Befehl ein: Smarorepory Rollback-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-rollbackhostost_with_target_Database

   Das folgende Beispiel zeigt den Befehl zum Rollback aller Zieldatenbanken, die auf hostA gemountet sind, und eine Repository-Datenbank namens repoA, die sich auf dem Repository-Host, repo_Host, befindet:

   ```
   smo repository rollback
       -repository
         -dbname repoA
         -host repo_host
         -login
          -username repouser
          -port 1521
        -rollbackhost hostA
   ```

2. Um ein Rollback auf mehreren Hosts durchzuführen, geben Sie den folgenden Befehl ein: Smarorpository Rollback-Repository-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username-portrepo_Port-rollbackhostost_with_Target_database1,Host_with_Target_database2

   > Geben Sie bei mehreren Hosts die durch Komma getrennten Hostnamen ein, und stellen Sie sicher, dass zwischen dem Komma und dem nächsten Hostnamen kein Platz vorhanden ist.Stellen Sie außerdem sicher, dass Sie den ganzen Satz von mehreren Hostnamen in doppelte Anführungszeichen eingeben.

   Das folgende Beispiel zeigt den Befehl zum Rollback aller Zieldatenbanken, die auf den Hosts gemountet sind, hostA, hostB und eine Repository-Datenbank namens repoA auf dem Repository-Host, repo_Host:

```
smo repository rollback
    -repository
      -dbname repoA
      -host repo_host
      -login
       -username repouser
       -port 1521
     -rollbackhost hostA,hostB
```

Die Hosts, Profile, Zeitpläne, Backups und Klone, die mit den Profilen der Zieldatenbanken für den Host verbunden sind, werden in das frühere Repository zurückgesetzt.

Verwandte Informationen

Voraussetzungen für die Durchführung eines Rollbacks

Aufgaben nach dem Rollback ausführen

Sie müssen einige weitere Schritte durchführen, nachdem Sie eine Repository-Datenbank zurückgesetzt und den SnapManager-Host von SnapManager 3.2 auf SnapManager 3.0 heruntergestuft haben, um die Zeitpläne anzuzeigen, die in der früheren Version der Repository-Datenbank erstellt wurden.

1. Navigieren Sie zu C:\Program Files\NetApp\SnapManager für Oracle\Repositorys.

   Das Repository-Verzeichnis kann zwei Dateien für jedes Repository enthalten. Der Dateiname mit dem Zahlenzeichen (#) wird mit SnapManager 3.1 oder höher erstellt und der Dateiname mit dem Bindestrich (-) wird mit SnapManager 3.0 erstellt.

   Die Dateinamen können wie folgt lauten:

   - Repository#SMO300a#SMOREPO1#10.72.197.141#1521
   - Repository-smo300a-smorepo1-10.72.197.141-1521
2. Ersetzen Sie das Zahlenzeichen (#) im Dateinamen durch den Bindestrich (-).

   Der Dateiname mit dem Zahlenzeichen (#) enthält jetzt Bindestrich (-): Repository-SMO300a-SMOREPO1-10.72.197.141-1521.

SnapManager wird konfiguriert

Nach der Installation von SnapManager müssen Sie je nach verwendeter Umgebung einige zusätzliche Konfigurationsaufgaben ausführen.

SnapManager-Konfigurationsparameter

SnapManager bietet eine Liste der Konfigurationsparameter, die Sie je nach Anforderung bearbeiten können. Die Konfigurationsparameter werden in der Datei smo.config

gespeichert. Die Datei smo.config enthält jedoch möglicherweise nicht alle unterstützten Konfigurationsparameter. Je nach Anforderung können Sie die Konfigurationsparameter hinzufügen.

In der folgenden Tabelle sind alle unterstützten SnapManager-Konfigurationsparameter aufgeführt und wird erläutert, wann diese Parameter verwendet werden können:

Parameter	Beschreibung
• Behalten.hourly.count • Beibehalten.hourly.duration • Behalten.monthly.count • Aufbewahrung.monatlich.Dauer	Diese Parameter legen die Aufbewahrungsrichtlinie fest, wenn Sie ein Profil erstellen. Sie können beispielsweise die folgenden Werte zuweisen:beibehalten.hourly.count = 12 Beibehalten.hourly.duration = 2 Behalten.monthly.count = 2 Aufbewahrung.monatlich.Dauer = 6
Restore.temporarVolumeName	Dieser Parameter weist dem temporären Volume einen Namen zu. Wenn SnapManager die indirekte Methode zur Wiederherstellung von Daten aus dem sekundären Storage verwendet, wird ein Scratch Volume auf dem primären Storage benötigt, um eine temporäre Kopie von Daten zu speichern, bis sie in die Datenbankdateien kopiert und die Datenbank wiederhergestellt wird. Es gibt keinen Standardwert. Wenn Sie keinen Wert angeben, müssen Sie einen Namen in den Wiederherstellungsbefehl eingeben, der die indirekte Methode verwendet. Sie können beispielsweise die folgenden Werte zuweisen:restore.temporaryVolumeName = smo_temp_Volume
Host.Credentials.persistent	Mit diesem Parameter kann SnapManager die Hostanmeldeinformationen speichern. Standardmäßig werden die Hostanmeldeinformationen nicht gespeichert. Die Hostanmeldeinformationen müssen jedoch gespeichert werden, wenn Sie über ein benutzerdefiniertes Skript verfügen, das auf einem Remote-Klon ausgeführt wird und Zugriff auf einen Remote-Server erfordert.Sie können das Speichern von Host-Anmeldeinformationen aktivieren, indem Sie Host.requeses.persist zuweisen. SnapManager verschlüsselt und speichert die Host-Anmeldedaten.

WiederherstellungPlanMaxFilesAbgespielt	Mit diesem Parameter können Sie die maximale Anzahl von Dateien festlegen, die in der Vorschau der Wiederherstellung angezeigt werden sollen.standardmäßig zeigt SnapManager maximal 20 Dateien in der Vorschau der Wiederherstellung an. Sie können jedoch in einen Wert größer 0 ändern. Sie können beispielsweise den folgenden Wert zuweisen: • WiederherstellungPlanMaxFilesAbgespielt = 30 Wenn Sie einen ungültigen Wert angeben, wird die Standardanzahl der Dateien angezeigt.
snapshot.list.Timeout.min	Mit diesem Parameter können Sie die Zeit in Minuten festlegen, für die SnapManager warten muss, bis der Befehl Snap list ausgeführt wird, wenn Sie SnapManager-Operationen ausführen.standardmäßig wartet SnapManager 30 Minuten. Sie können jedoch in einen Wert größer 0 ändern. Sie können beispielsweise den folgenden Wert zuweisen: • snapshot.list.Timeout.min = 40 Wenn Sie einen ungültigen Wert angeben, wird der Standardwert verwendet. Wenn die Ausführungszeit des Befehls Snap list bei jedem SnapManager-Vorgang den Wert überschreitet, der Snapshot.list.Timeout.min zugewiesen ist, schlägt der Vorgang mit einer Zeitüberschreitung fehl.

PruneIfFileExistsInOtherDestination	Mit diesem Beschneidungsparameter können Sie das Ziel der Archiv-Log-Dateien definieren. Die Archivprotokolldateien werden in mehreren Zielorten gespeichert. Beim Beschneiden von Archiv-Log-Dateien muss SnapManager das Ziel der Archiv-Log-Dateien kennen. Sie können folgende Werte zuweisen: • Wenn Sie die Archiv-Log-Dateien von einem bestimmten Ziel aus pruneIfFileExistsInOtherDestination löschen möchten, müssen Sie pruneIfFileExistsInOtherDestination false zuweisen. • Wenn Sie die Archiv-Log-Dateien von einem externen Ziel aus pruneIfFileExistsInOtherDestination löschen möchten, müssen Sie true zu pruneIfFileExistsInOtherDestination zuweisen.
prune.archivelogs.backedup.from.otherdestination	Mit diesem Beschneider-Parameter können Sie die Archivprotokolldateien, die von den angegebenen Archivprotokollzielen gesichert oder von externen Archivprotokollzielen gesichert wurden, beschneiden. Sie können folgende Werte zuweisen: • Wenn Sie die Archivprotokolldateien aus den angegebenen Zielen beschneiden und wenn die Archivprotokolldateien von den angegebenen Zielen mithilfe von -prune-dest gesichert werden, müssen Sie false prune.archivelogs.backedup.from.otherdestination zuweisen. • Wenn Sie die Archivprotokolldateien von angegebenen Zielen beschneiden und die Archivprotokolldateien mindestens einmal von einem der anderen Ziele gesichert werden sollen, müssen Sie True prune.archivelogs.backedup.from.otherdestination zuweisen.

Maximum.archivolog.files.toprune.atATIME	Mit diesem Beschneider-Parameter können Sie die maximale Anzahl von Archivprotokolldateien definieren, die Sie zu einem bestimmten Zeitpunkt beschneiden können. Sie können beispielsweise den folgenden Wert zuweisen:maximum.archivelog.files.toprune.atATIME = 998 Der Wert, der maximal.archivolog.files.toprune.atatime zugewiesen werden kann, muss kleiner als 1000 sein.
Archivprotokolle.konsolidieren	Mit diesem Parameter kann SnapManager die doppelten Archiv-Log-Backups freigeben, wenn Sie true dem archivelogs.Consolidate zuweisen.
Suffix.Backup.Label.with.logs	Mit diesem Parameter können Sie das Suffix angeben, das Sie hinzufügen möchten, um die Namen der Bezeichnungen der Datensicherung und des Archiv-Log-Backups zu unterscheiden.zum Beispiel, wenn Sie Logs dem Suffix.Backup.Label.with.logs zuweisen, wird _logs als Suffix zum Backup-Label des Archivprotokolls hinzugefügt. Das Backup-Label für das Archivprotokoll wäre dann ARCH_logs.
backup.archivelogs.beyond.missingfiles	Mit diesem Parameter kann SnapManager die fehlenden Archivprotokolldateien in die Sicherung aufnehmen. Die Archivprotokolldateien, die nicht im aktiven Dateisystem vorhanden sind, sind nicht im Backup enthalten. Wenn Sie alle Archivprotokolldateien einschließen möchten, auch jene, die nicht im aktiven Dateisystem vorhanden sind, müssen Sie True backup.archivelogs.beyond.missingfiles zuweisen. Sie können FALSE zuweisen, um die fehlenden Archivprotokolldateien zu ignorieren.
Srvctl.Timeout	Mit diesem Parameter können Sie den Timeout-Wert für den srvctl-Befehl definieren. **Hinweis:** die Serversteuerung (SRVCTL) ist ein Dienstprogramm zur Verwaltung von RAC-Instanzen. Wenn SnapManager mehr Zeit in Anspruch nimmt, um den srvctl-Befehl auszuführen als den Timeout-Wert, schlägt der SnapManager-Vorgang mit dieser Fehlermeldung fehl: Fehler: Timeout ist beim Ausführen des Befehls srvctl-Status aufgetreten.

snapshot.restore.storageNameCheck	Mit diesem Parameter kann SnapManager den Wiederherstellungsvorgang mit Snapshot Kopien durchführen, die vor der Migration von Data ONTAP im 7-Mode zu Clustered Data ONTAP erstellt wurden. Der dem Parameter zugewiesene Standardwert ist false. Wenn Sie von Data ONTAP 7-Mode zu Clustered Data ONTAP migriert haben, die Snapshot Kopien jedoch vor der Migration verwenden möchten, legen Sie den Wert für Snapshot.restore.storageNameCheck=true fest.
services.common.disableAbort	Dieser Parameter deaktiviert die Bereinigung bei einem Ausfall lang laufender Vorgänge. Wenn Sie services.common.disableAbort=true.For beispielsweise einen Klonvorgang ausführen, der lange dauert und dann aufgrund eines Oracle-Fehlers fehlschlägt, sollten Sie den Klon möglicherweise nicht bereinigen. Wenn Sie services.common.disableAbort=true festlegen, wird der Klon nicht gelöscht. Sie können das Oracle Problem beheben und den Klonvorgang ab dem Fehlerpunkt neu starten.
• Backup.Sleep.dnfs.Layout • backup.sleep.dnfs.secs	Diese Parameter aktivieren den Schlafmechanismus im Direct NFS Layout (dNFS). Nachdem Sie die Datensicherung der Kontrolldateien mit dNFS oder einem Network File System (NFS) erstellt haben, versucht SnapManager, die Kontrolldateien zu lesen, aber die Dateien werden möglicherweise nicht gefunden.um den Sleep-Mechanismus zu aktivieren, stellen Sie sicher, dass Backup.Sleep.dnfs.Layout=true. Der Standardwert ist true. Wenn Sie den Schlafmechanismus aktivieren, müssen Sie die Schlafdauer backup.sleep.dnfs.secs zuweisen. Die zugewiesene Schlafzeit ist in Sekunden und der Wert hängt von Ihrer Umgebung ab. Der Standardwert ist 5 Sekunden. Beispiel: • Backup.Sleep.dnfs.Layout=true • backup.sleep.dnfs.secs=2

• override.default.backup.pattern • new.default.backup.pattern	Wenn Sie das Backup-Label nicht angeben, erstellt SnapManager ein Standard-Backup-Label. Mit diesen SnapManager-Parametern können Sie das Standard-Backup-Label anpassen.um die Anpassung des Backup-Labels zu ermöglichen, stellen Sie sicher, dass der Wert override.default.backup.pattern auf true gesetzt ist. Der Standardwert ist false. Um das neue Muster des Backup-Labels zuzuweisen, können Sie Schlüsselwörter wie Datenbankname, Profilname, Umfang, Modus und Hostname new.default.backup.pattern zuweisen. Die Stichwörter sollten mit einem Unterstrich getrennt werden. Beispiel: new.default.backup.pattern=dbname_profile_hostname_scope_mode. Der Zeitstempel wird automatisch am Ende des generierten Etiketts eingefügt.
allow.underscore.in.clone.sid	Oracle unterstützt die Verwendung des Unterstreichung in Clone SID von Oracle 11gR2. Mit diesem SnapManager-Parameter können Sie einen Unterstrich in den Namen Clone SID einfügen.um einen Unterstrich in den Clone SID-Namen einzuschließen, stellen Sie sicher, dass der Wert allow.underscore.in.clone.sid auf true gesetzt ist. Der Standardwert ist true. Wenn Sie eine Oracle-Version vor Oracle 11gR2 verwenden oder keinen Unterstrich in den Namen Clone SID aufnehmen möchten, setzen Sie den Wert auf false.
oracle.parameters.with.comma	Mit diesem Parameter können Sie alle Oracle-Parameter angeben, die Komma (,) als Wert haben.während einer Operation verwendet SnapManager oracle.parameters.with.comma, um alle Oracle-Parameter zu überprüfen und die Aufteilung der Werte zu überspringen. Wenn z. B. der Wert von nls_numeric_characters=, angegeben wird, geben Sie dann oracle.parameters.with.comma=nls_numeric_characters an. Wenn mehrere Oracle-Parameter mit Komma als Wert vorhanden sind, müssen Sie alle Parameter in oracle.parameters.with.comma angeben.

• ArchivLogs.exclude • ArchivedLogs.exclude.fileslike • <db-unique-Name>.archivedLogs.exclude.fileslike	Diese Parameter erlauben es SnapManager, die Archivprotokolldateien von den Profilen und Backups auszuschließen, wenn sich die Datenbank nicht auf einem Speichersystem befindet, das mit Snapshot Kopien aktiviert ist, und Sie SnapManager-Vorgänge auf diesem Speichersystem ausführen möchten.**Hinweis:** vor der Erstellung eines müssen Sie die Ausschlussparameter in die Konfigurationsdatei einfügen Profil: Die diesen Parametern zugewiesenen Werte können entweder ein Verzeichnis der obersten Ebene oder ein Mount-Punkt sein, an dem die Archivprotokolldateien vorhanden sind, oder ein Unterverzeichnis. Um die Archivprotokolldateien von der Integration im Profil und der Sicherung auszuschließen, müssen Sie einen der folgenden Parameter angeben: • ArchivedLogs.exclude, um einen regulären Ausdruck für das Ausschließen von Archiv-Log-Dateien aus allen Profilen oder Backups anzugeben. Die Archivprotokolldateien, die dem regulären Ausdruck entsprechen, werden von allen Profilen und Backups ausgeschlossen. Zum Beispiel können Sie archivedLogs.exclude = J:\\ARCH\\.* einstellen. Wenn das Ziel ein Dateitrennzeichen hat, muss dem Muster ein zusätzliches Schrägungssymbol (\) hinzugefügt werden, und das Muster muss mit einem Doppelschrägstrich-Muster (\\.*) enden. • ArchivedLogs.exclude.filesWie geben Sie einen SQL-Ausdruck an, um Archivprotokolldateien von allen Profilen oder Backups auszuschließen. Die Archivprotokolldateien, die dem SQL-Ausdruck entsprechen, werden von allen Profilen und Backups ausgeschlossen. Sie können zum Beispiel archivedLogs.exclude.fileslike = J:\\ARCH2\\% festlegen.

	• <db-unique-Name>.archivedLogs.exclude.filesWie geben Sie einen SQL-Ausdruck an, um Archivprotokolldateien ausschließlich aus dem Profil oder dem Backup auszuschließen, das für die Datenbank mit dem angegebenen db-Unique-Namen erstellt wurde. Die Archivprotokolldateien, die dem SQL-Ausdruck entsprechen, werden vom Profil und den Backups ausgeschlossen. Sie können beispielsweise mydb.archivedLogs.exclude.fileslike = J:\\ARCH2\\% festlegen. Wenn das Ziel über ein Dateitrennzeichen verfügt, muss dem Muster ein zusätzliches Schrägungssymbol (\) hinzugefügt werden, und das Muster muss mit einem Doppelschrägstrich-Muster (\\%) enden.

Bearbeiten der Konfigurationsparameter

Je nach Umgebung können Sie die Standardwerte ändern, die dem Konfigurationsparameter zugewiesen sind.

1. Öffnen Sie die Konfigurationsdatei vom folgenden Standardspeicherort:

   Standardinstallationsverzeichnis\Properties\smo.config

2. Ändern Sie die Standardwerte der Konfigurationsparameter.

   Sie können auch unterstützte Konfigurationsparameter hinzufügen, die nicht in der Konfigurationsdatei enthalten sind, und ihnen Werte zuweisen.

3. Starten Sie den SnapManager für Oracle Server neu.

Starten von SnapManagerfür Oracle

Im Abschnitt „SnapManager-Start“ werden die Aufgaben aufgeführt, die Sie beim Start von SnapManager ausführen. Verwenden Sie diesen Abschnitt auch, wenn Sie nur über SnapManager lernen.

Vor der Verwendung von SnapManager sollten Sie die folgenden Aktionen durchgeführt haben:

- Die SnapManager Software wurde heruntergeladen und installiert.

- Sie haben festgelegt, ob die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle verwendet werden sollen.

Identifizieren einer vorhandenen Datenbank für das Backup

Sie können die Systemkennung (SID) der SnapManager-Datenbank identifizieren, die bei der Erstellung eines Profils verwendet wird.

Die Standard-Oracle-Benutzer-ID für nicht-SAP-Systeme ist oracle.

1. Klicken Sie Auf **Start** > **Systemsteuerung** > **Verwaltung** > **Services**.
2. Überprüfen Sie den Oracle-Service OracleServiceSID.

   Wenn der Dienst OracleServiceFASDB genannt wird, ist die Datenbank-SID FASDB.

Überprüfen des Oracle Listener-Status

Sie können den Oracle-Listener-Status mit dem Status-Befehl lsnrctl überprüfen.

- Sie müssen eine Verbindung zur Datenbank herstellen.

Eine standardmäßige Oracle-Installation setzt den Listener-Port der Datenbank auf 1521.

1. Geben Sie an der Eingabeaufforderung den Status:lsnrctl ein

Erstellen von Oracle-Benutzern für die Repository-Datenbank

Sie können einen Oracle-Benutzer für die Repository-Datenbank erstellen und bestimmte Berechtigungen zuweisen, um verschiedene Vorgänge in der Repository-Datenbank auszuführen.

Sie müssen dem Oracle-Benutzer die Verbindungsberechtigungen und Ressourcenberechtigungen zuweisen. Sie müssen keinen Benutzer für die Repository-Datenbank mit sysdba-Berechtigungen erstellen.

Sie müssen jedoch einen Oracle-Benutzer mit der sysdba-Rolle für die Zieldatenbank erstellen.

1. Melden Sie sich bei SQL *Plus an.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: Sqlplus '/ AS sysdba'

```
SQL*Plus: Release 11.2.0.1.0 Production on Wed Jun 1 06:01:26 2011
Copyright (c) 1982, 2009, Oracle.  All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Automatic Storage Management, OLAP, Data Mining
and Real Application Testing options
```

2. Um einen Benutzer zu erstellen, z. B. repo1_user, geben Sie für das Repository mit dem Administrator-Passwort, z. B. adminpw1, den folgenden Befehl an der SQL-Eingabeaufforderung ein: SQL> create user

repo1_user, der von adminpw1 identifiziert wurde;

3. Um dem Benutzer Verbindungsberechtigungen und Ressourcenberechtigungen zu gewähren, geben Sie den folgenden Befehl ein: Erteilen Sie eine Verbindung, Ressource für repo1_user;

Erstellen eines Oracle-Benutzers für die Zieldatenbank

Sie müssen einen Oracle-Benutzer mit der sysdba-Rolle erstellen, die eine Verbindung zur Datenbank herstellt und Datenbankvorgänge durchführt.

SnapManager kann jeden Oracle-Benutzer mit sysdba-Berechtigungen verwenden, die in der Zieldatenbank vorhanden sind, zum Beispiel den Standardbenutzer „sys“. Sie können auch einen Benutzer in der Zieldatenbank erstellen, der ausschließlich von SnapManager verwendet werden soll.

1. Melden Sie sich bei SQL *Plus an.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: Sqlplus '/ AS sysdba'

2. Um einen Benutzer zu erstellen, zum Beispiel smo_oper mit dem Administrator-Passwort, zum Beispiel adminpw1, geben Sie an der SQL-Eingabeaufforderung den folgenden Befehl ein: SQL> Benutzer erstellen smo_oper identifiziert durch adminpw1;
3. Gewähren sie dem Oracle-Benutzer sysdba-Berechtigungen durch Eingabe des folgenden Befehls: SQL> Grant sysdba to smo_oper;

Zugriff auf SnapManager

Der Zugriff auf SnapManager erfolgt entweder über die Befehlszeilenschnittstelle (CLI) oder über die grafische Benutzeroberfläche (GUI).

Sie haben folgende Möglichkeiten, verschiedene SnapManager-Vorgänge auszuführen:

- Durch Eingabe von Befehlen in der CLI auf einem Host, der sich im gleichen Netzwerk wie der Datenbank-Host befindet.

  Eine Liste aller Befehle und eine Erläuterung ihrer Optionen und Argumente finden Sie im Kapitel Command Reference.

  Um auf die CLI zuzugreifen, klicken Sie **Start** > **Alle Programme** > **NetApp** > **SnapManager für Oracle** > **Starten Sie die SMO Befehlszeilenschnittstelle (CLI)**.

- Durch Zugriff auf die GUI auf einem Host in demselben Netzwerk wie der Datenbank-Host.

  Die GUI bietet einfache und benutzerfreundliche Assistenten, mit denen Sie verschiedene Aufgaben ausführen können.

Verwandte Informationen

Befehlsreferenz für SnapManager für Oracle

Starten des SnapManager-Hostservers

Sie können den SnapManager-Server mithilfe der Windows-Dienste starten.

1. Klicken Sie Auf **Start** > **Systemsteuerung** > **Verwaltung** > **Services**.
2. Wählen Sie im Fenster Services NetAppSnapManager 3.3 fürOracle aus.
3. Sie können den Server auf drei Arten starten:
   - Klicken Sie im linken Bereich auf **Start**.
   - Klicken Sie mit der rechten Maustaste auf NetAppSnapManager 3.3 für Oracle und wählen Sie im Dropdown-Menü die Option **Start** aus.
   - Doppelklicken Sie auf NetAppSnapManager 3.3 für Oracle, und klicken Sie dann im Fenster Eigenschaften auf **Start**.

Überprüfen des SnapManager-Hostserverstatus

Der Server muss ausgeführt werden, damit Sie Befehle ausführen oder SnapManager Vorgänge initiieren können. Sie müssen den Status des Servers überprüfen, bevor Sie Vorgänge ausführen.

1. Wählen Sie im Fenster Dienste SnapManager 3.3 forOracle aus.
2. Zeigen Sie den Status in der Spalte Status an.

Mit SnapManager-Befehlen

Nachdem Sie den SnapManager-Hostserver gestartet haben, können Sie SnapManager verwenden, indem Sie Befehle an der Eingabeaufforderung auf Ihrem Host eingeben.

1. So führen Sie einen Vorgang aus:
   - Im Falle eines Windows Hosts gehen Sie zu **Start** > **Alle Programme** > **NetApp** > **SnapManager für Oracle** > **Start SMO Command Line Interface (CLI)**

Starten der SnapManager GUI

Wenn SnapManager auf dem Host installiert ist, starten Sie die grafische Benutzeroberfläche (GUI) für SnapManager, indem Sie das Programm aus einer Liste von Programmen auswählen.

- Stellen Sie sicher, dass der SnapManager-Server gestartet wird.

Sie können die SnapManager GUI auf eine der folgenden Arten starten:

- Klicken Sie im SnapManager Host auf **Start** > **Alle Programme** > **NetApp** > **SnapManager für Oracle** > **Start SMO GUI**.
- Wenn SnapManager nicht auf dem Host installiert ist, verwenden Sie Java Web Start, der SnapManager-Komponenten herunterlädt und die GUI startet.

Verwandte Informationen

Herunterladen und Starten der grafischen Benutzeroberfläche mit Java Web Start

Herunterladen und Starten der grafischen Benutzeroberfläche mit Java Web Start

Sie können Java Web Start verwenden, wenn SnapManager nicht auf dem Host installiert

ist. Java Web Start lädt SnapManager-Komponenten herunter und startet die grafische Benutzeroberfläche (GUI). Die unterstützten JRE-Versionen sind 1.5, 1.6, 1.7 und 1.8.

Sie müssen sicherstellen, dass die folgenden Bedingungen erfüllt sind:

- Der SnapManager Server wird ausgeführt.
- Ein Webbrowser-Fenster ist geöffnet.

a. Geben Sie im Web-Browser-Fenster von Microsoft Internet Explorer ein https://smo-server.domain.com:port.

   smo-server.domain.com ist der vollqualifizierte Host-Name und die Domäne, auf der Sie SnapManager installiert haben, und Port ist der Listening-Port für den SnapManager-Server (standardmäßig 27214).

   Sie müssen https im Browserfenster eingeben.

   Ein Dialogfeld mit der Meldung Es gibt ein Problem mit dem Sicherheitszertifikat der Website… möchten Sie fortfahren? Wird angezeigt.

b. Klicken Sie auf **Ja** oder **Weiter**.

c. Klicken Sie auf den Link Klicken Sie hier, um JRE 6.0 und die Anwendung herunterzuladen und zu installieren.

   Ein Link mit der Bezeichnung Download Java Web Start mit der Nachricht Diese Website benötigt möglicherweise das folgende ActiveX-Steuerelement: Java Plug-in 1.6"… „Klicken Sie hier, um die Installation anzuzeigen.

d. Führen Sie im Fenster Installieren die folgenden Schritte aus:

   i. Klicken Sie auf die Nachricht mit der Beschriftung Klicken Sie hier, um… zu installieren

      Es wird ein Menü **ActiveX-Steuerelement installieren** angezeigt.

   ii. Wählen Sie **ActiveX-Steuerelement installieren…**.

      Die Nachricht Internet Explorer - Sicherheitswarnung mit folgendem Text: "Möchten Sie diese Software installieren? Name: Java Plug-in 1.6 wird angezeigt.

   iii. Klicken Sie Auf **Installieren**.

      Es wird ein Fenster „Java Plug-in 1.6.“ für das Installationsprogramm für J2SE Runtime Environment 1.6 angezeigt.

   iv. Klicken Sie Auf **Installieren**.

   Es wird ein Fenster angezeigt, in dem Sie aufgefordert werden, J2SE Runtime Environment 1.6 zu installieren.

e. Führen Sie im Fenster Installieren die folgenden Schritte aus:

   i. Wählen Sie auf der Seite Lizenzvereinbarung die Option **Ich akzeptiere die Bedingungen in der Lizenzvereinbarung** und klicke auf **Weiter**.

   ii. Wählen Sie auf der Seite Einrichtungstyp die Option **typisch** aus, und klicken Sie auf **Weiter**.

   iii. Klicken Sie im Fenster Installation abgeschlossen auf **Fertig stellen**.

SnapManager beginnt herunterzuladen.

Dialogfeld „Datei herunterladen“ mit der Meldung Möchten Sie diese Datei speichern? Application.jnlp wird angezeigt.

f. Führen Sie im Datei-Download-Fenster die folgenden Schritte aus:
   i. Installieren Sie die neueste Version von JRE 1.6 auf dem Windows-Client.
   ii. Überprüfen Sie, ob Java installiert ist, indem Sie den folgenden Befehl ausführen: java -Version

       Die Ausgabe sollte Java-Version 1.6.0_24 (Java 1.6) oder höher angeben.

   iii. Ändern Sie Ihre Windows-Konfigurationseinstellungen, um immer Dateien mit der Erweiterung jnlp mit dem Programm Java Web Start Launcher zu öffnen.

       Die Schritte zum Ändern der Windows-Konfigurationseinstellungen variieren je nach der verwendeten Windows-Version.

   iv. Geben Sie die SnapManager-URL ein, die Sie in Schritt 1 angegeben haben.

       Der Download von SnapManager startet auf dem Windows-Client und ein Dialogfeld Warnung - Sicherheit wird angezeigt.

g. Führen Sie die folgenden Schritte aus.

   Der Inhalt der Meldungen und die Beschriftungen der Schaltflächen variieren je nach Plattform.

   i. Klicken Sie im Dialogfeld Warnung - Sicherheit auf **Ja**.

       Ein Dialogfeld wird angezeigt.

   ii. Klicken Sie im Dialogfeld „nicht übereinstimmende Hostnamen“ auf **Ausführen**.

       Das Dialogfeld Warnung - Sicherheit mit einer Meldung über die Signatur der SnapManager-Anwendung wird angezeigt.

   iii. Klicken Sie Auf **Ausführen**.

       Ein Dialogfeld mit dem Titel Java Installer – Sicherheitswarnung und der Meldung Sicherheit - die digitale Signatur der Anwendung weist einen Fehler auf. Soll die Anwendung ausgeführt werden, wird angezeigt.

   iv. Klicken Sie Auf **Ausführen**.

       Der Browser lädt die Benutzeroberfläche von SnapManager für Oracle herunter und startet sie.

Überprüfen der Umgebung

Sie können die Umgebung überprüfen, um sicherzustellen, dass SnapDrive und SnapManager korrekt eingerichtet sind.

Laden Sie die erforderlichen Voraussetzungen herunter, installieren Sie sie und richten Sie sie ein. Stellen Sie sicher, dass SnapManager installiert ist und der Host-Server ausgeführt wird.

1. Führen Sie den folgenden Befehl:smo System verify aus, um zu überprüfen, ob SnapDrive installiert ist und über das Root-Konto ausgeführt werden kann

Verwandte Informationen

Der Befehl smo System verify

Überprüfen von SnapDrive für Windows

Wenn Sie SnapDrive für Windows installiert haben, vergewissern Sie sich, dass Sie vor der Verwendung von SnapManager eine Snapshot Kopie erstellen können.

1. Klicken Sie im Startmenü mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie **Verwalten**.
2. Klicken Sie im Fenster Computerverwaltung auf **Speicherung** > **SnapDrive**.
3. Wählen Sie ein Laufwerk aus.

   Weitere Informationen zur Verwendung von SnapDrive finden Sie im *SnapDrive for Windows Installation and Administration Guide*.

   Wenn Sie erfolgreich Festplatteninformationen für das SnapDrive Produkt gefunden haben, funktioniert SnapDrive ordnungsgemäß.

Verwandte Informationen

"*SnapDrive for Windows Installation and Administration Guide*: mysupport.netapp.com/documentation/productsatoz/index.html"

Repositories werden erstellt

SnapManager benötigt ein Repository auf einem Host, um Daten über die von Ihnen ausgeführten Vorgänge abzuhalten.

Stellen Sie sicher, dass die folgenden Aufgaben abgeschlossen sind:

1. Erstellen Sie einen Oracle-Benutzer und ein Kennwort in der Repository-Datenbank.
2. Benutzerzugriff auf das Repository autorisieren.

Für ein Repository benötigt SnapManager für Oracle mindestens 4-KB-Blockgrößen für die Tablespaces, in denen er installiert ist. Sie können die Blockgröße mithilfe des folgenden SQL-Befehls überprüfen:

```
select a.username, a.default_tablespace, b.block_size
from dba_users a, dba_tablespaces b
a.username = repo_user
```

Wo

- a.default_tablespace = b.tabespace_Name
- a.username = Benutzername im Repository

Wenn Sie Repositorys aktualisieren, müssen Sie den SnapManager-Server neu starten, um die zugehörigen Zeitpläne neu zu starten.

1. Um das Repository zu erstellen, geben Sie den Befehl Repository create unter Verwendung des folgenden allgemeinen Formats ein: bbs Repository create -Repository -dbname repo_Service_Name -Host repo_Host -Login -username repo_username -Port repo_Port-Force] [-noprompt] [-quiet

   Wo?

   - -Repository -dbname ist der Name der Repository-Datenbank.
   - -Host ist der Name des Hosts für das Repository.
   - -Username ist der Name des Datenbankbenutzers, der Zugriff auf das Repository hat.
   - -Port ist der Port für den Host. Weitere Optionen für diesen Befehl:

     [-Force] [-noprompt]

   + HINWEIS: Wenn Sie ein Repository mit demselben Namen haben und die Option -Force verwenden, werden alle Daten in einem vorhandenen Repository-Schema überschrieben.

Erstellen eines Repository

Mit der folgenden Befehlszeile wird ein Repository erstellt.

```
smo repository create -repository -dbname HRDP
-host server1 -login -username admin -port 1521
```

So organisieren Sie Repositories

Organisieren Sie die SnapManager Repositorys, um Ihre Geschäftsanforderungen zu erfüllen. Sie können sie auf verschiedene Arten organisieren, einschließlich nach Anwendungstyp und Nutzung.

Sie können Repositories auf verschiedene Weise organisieren. Dabei gibt es zwei Möglichkeiten:

Typ	Merkmale

Nach Applikation	Wenn bei Ihnen mehrere Oracle Datenbanken unterschiedliche Applikationen ausgeführt werden, können Sie für jeden Applikationstyp ein SnapManager-Repository erstellen. Jedes SnapManager-Repository hätte Profile für die Datenbanken eines bestimmten Applikationstyps. Alle Produktions-, Entwicklungs- und Testdatenbanken dieses Applikationstyps werden durch dasselbe SnapManager Repository gemanagt. Mit dieser Option lassen sich ähnliche Datenbanken gruppieren und das Klonen einfacher vereinfachen. Wenn Sie jedoch verschiedene Applikationstypen haben, müssen Sie möglicherweise mehrere SnapManager-Repositorys verwalten. Wenn Sie sich für die Implementierung eines anderen Applikationstyps entscheiden, müssen Sie ein weiteres SnapManager-Repository erstellen. Da diese SnapManager Repositorys Produktionsdatenbanken managen, müssen sich alle diese Repositorys auf einem Server mit hoher Verfügbarkeit befinden, was zu teuer sein kann. Zusätzlich kann es Sicherheitsproblem geben, dass die Produktionsdatenbanken sowie Entwicklungs- und Test-Datenbanken desselben Typs im SnapManager Repository gemanagt werden müssen.
Nach Verwendung	Sie können die Datenbanken je nach Nutzung (z. B. Produktion, Entwicklung, Tests und Training) zwischen den SnapManager Repositorys verteilen. Mit dieser Option wird die Anzahl der Repositorys auf die verschiedenen Datenbanktypen beschränkt, über die Sie verfügen. Da alle Produktionsdatenbanken von einem einzigen SnapManager-Repository gemanagt werden würden, können nur Administratoren der Produktionsdatenbank für den Zugriff auf das Repository erhalten werden. Wenn Sie eine weitere Datenbank für einen neuen Anwendungstyp bereitstellen möchten, müssen Sie die Datenbank nur im entsprechenden SnapManager-Repository registrieren, anstatt ein neues Repository zu erstellen. Hochverfügbarkeit ist nur für das SnapManager-Repository möglich, das die Profile aller Produktionsdatenbanken enthält.

SnapManager für Oracle und SnapManager für SAP sollten nicht dasselbe Repository gemeinsam nutzen. Bei SnapManager für Oracle und SnapManager für SAP müssen Sie für jedes Produkt ein anderes Repository (ein anderer Oracle Datenbankbenutzer) verwenden, sofern Sie beide in Ihrer Umgebung vorhanden sind. Durch die Verwendung eines anderen Repositorys, entweder in derselben oder in unterschiedlichen Datenbanken, werden mehr Flexibilität durch unabhängige Upgrade-Zyklen für jedes Produkt ermöglicht.

Reihenfolge der Durchführung von Vorgängen

SnapManager ermöglicht Ihnen die Durchführung verschiedener Aufgaben, z. B. das Erstellen von Profilen, das Durchführen von Backups und das Klonen von Backups. Diese Vorgänge müssen in einer bestimmten Reihenfolge ausgeführt werden.

1. Erstellen Sie ein Profil in einem vorhandenen Repository mithilfe des Befehls smoprofile create.

   Der für die Zieldatenbank angegebene Oracle-Benutzer muss über sysdba-Berechtigungen verfügen.

   Im folgenden Beispiel wird der Befehl zum Erstellen eines Profils gezeigt:

   ```
   smo profile create -profile prof1 -profile-password prof1cred
   -repository -dbname HR1 -login -username admin -host server1 -port 1521
   -database -dbname dedb -login -username db_oper2
   -password dbpw1 -host server1 -port 1521
   ```

2. Erstellen Sie ein Backup auf einem vorhandenen Profil mit dem smo Backup create Befehl.

   Im folgenden Beispiel wird der Befehl zum Erstellen eines Backups gezeigt:

   ```
   smo backup create -profile prof1 -full -offline -label full_backup_prof1
   -force
   ```

3. Wiederherstellung eines Datenbank-Backups auf dem Primär-Storage mithilfe des smo Backup-Restore-Befehls

   Das folgende Beispiel zeigt den Befehl zum Wiederherstellen eines Backups:

   ```
   smo backup restore -profile prof1 -label full_backup_prof1
   -complete -recover -alllogs
   ```

4. Erstellen Sie mit dem Befehl smo Clone template eine Klonspezifikation.

   Sie können den Klon-Assistenten in der grafischen Benutzeroberfläche (GUI) verwenden, um eine Spezifikation für das Klonen einer Vorlage zu erstellen. Sie können die Klon-Spezifikationsdatei auch mit einem Texteditor erstellen.

5. Klonen einer Datenbank mit einem vorhandenen Backup mit dem Befehl zum Erstellen von smo Clone.

   Sie müssen über eine vorhandene Klonspezifikation verfügen oder eine Klonspezifikation erstellen, um die Storage- und Datenbank-Spezifikationen für den Klon anzugeben.

   Im folgenden Beispiel wird der Befehl zum Erstellen eines Klons angezeigt:

```
smo clone create -profile prof1 -backup-label full_backup_prof1
-newsid clone1 -label prof1_clone -clonespec
C:\\clone_spec\\prof1_clonespec.xml
```

Sicherheits- und Anmeldeinformationsmanagement

Sie können die Sicherheit in SnapManager durch Benutzerauthentifizierung verwalten. Die Benutzerauthentifizierungsmethode ermöglicht den Zugriff auf Ressourcen wie Repositorys, Hosts und Profile.

Wenn Sie einen Vorgang über die Befehlszeilenschnittstelle (CLI) oder die grafische Benutzeroberfläche (GUI) ausführen, ruft SnapManager die für Repositorys und Profile festgelegten Anmeldeinformationen ab. SnapManager speichert Anmeldeinformationen früherer Installationen.

Das Repository und die Profile können mit einem Passwort gesichert werden. Eine Anmeldeinformationen ist das für den Benutzer für ein Objekt konfigurierte Passwort, und das Passwort ist nicht für das Objekt selbst konfiguriert.

Sie können die Authentifizierung und Anmeldeinformationen verwalten, indem Sie die folgenden Aufgaben ausführen:

- Verwalten Sie die Benutzerauthentifizierung entweder durch Eingabeaufforderungen für Passwörter für Vorgänge oder mithilfe des Befehls smo Credential Set.

  Legen Sie Anmeldedaten für ein Repository, einen Host oder ein Profil fest.

- Zeigen Sie die Anmeldeinformationen an, die die Ressourcen regeln, auf die Sie Zugriff haben.
- Löschen Sie die Anmeldeinformationen eines Benutzers für alle Ressourcen (Hosts, Repositorys und Profile).
- Löschen Sie die Anmeldeinformationen eines Benutzers für einzelne Ressourcen (Hosts, Repositorys und Profile).

> Wenn sich die Repository-Datenbank auf einem Windows-Host befindet, müssen sowohl der lokale Benutzer als auch der Domänenbenutzer über dieselben Anmeldeinformationen verfügen.

Was ist die Benutzerauthentifizierung

SnapManager authentifiziert den Benutzer mithilfe einer Betriebssystemanmeldung auf dem Host, auf dem der SnapManager-Server ausgeführt wird. Sie können die Benutzerauthentifizierung entweder durch Passwortaufforderungen zu Vorgängen oder durch Verwendung der Smo-Anmeldeinformationen aktivieren. Sie können die Benutzerauthentifizierung entweder durch Eingabeaufforderungen zum Passwort oder über den Befehl smo-Anmeldeinformationssatz aktivieren.

Die Anforderungen an die Benutzerauthentifizierung hängen davon ab, wo der Vorgang ausgeführt wird.

- Wenn sich der SnapManager-Client auf demselben Server wie der SnapManager-Host befindet, werden Sie durch die BS-Anmeldedaten authentifiziert.

  Sie werden nicht zur Eingabe eines Passworts aufgefordert, da Sie bereits beim Host angemeldet sind, auf dem der SnapManager-Server ausgeführt wird.

- Wenn der SnapManager-Client und der SnapManager-Server auf verschiedenen Hosts sind, muss SnapManager Sie mit beiden OS-Anmeldedaten authentifizieren.

  SnapManager fordert Sie zur Eingabe von Passwörtern für jeden Vorgang auf, wenn Sie Ihre BS-Anmeldeinformationen nicht im SnapManager-Benutzereinweiscache gespeichert haben. Wenn Sie den Befehl smo causendential set -Host eingeben, speichern Sie die OS-Anmeldeinformationen in der SnapManager-Anmeldeinformationscache-Datei und so fordert SnapManager nicht zur Eingabe des Passworts für einen Vorgang auf.

Wenn Sie mit dem SnapManager-Server authentifiziert sind, gelten Sie als effektiver Benutzer. Der effektive Benutzer für einen Vorgang muss ein gültiges Benutzerkonto auf dem Host sein, auf dem der Vorgang ausgeführt wird. Wenn Sie beispielsweise einen Klonvorgang ausführen, sollten Sie sich beim Ziel-Host für den Klon einloggen können.

SnapManager für Oracle kann die Autorisierung von Benutzern, die in zentralen Active Directory-Diensten erstellt wurden, z. B. LDAP und ADS, möglicherweise nicht unterstützen. Um sicherzustellen, dass die Authentifizierung nicht fehlschlägt, müssen Sie die konfigurierbare auth.diableServerAuthorization auf true setzen.

Als effektiver Benutzer können Sie die Anmeldeinformationen folgendermaßen verwalten:

- Optional können Sie SnapManager so konfigurieren, dass Benutzeranmeldeinformationen in der SnapManager-Benutzeranmeldedatei gespeichert werden.

  Standardmäßig werden in SnapManager keine Host-Anmeldedaten gespeichert. Sie können dies ändern, beispielsweise, wenn Sie benutzerdefinierte Skripte haben, die Zugriff auf einen Remote-Host benötigen. Der Remote-Klonvorgang ist ein Beispiel für eine SnapManager-Operation, die die Anmeldedaten eines Benutzers für einen Remote-Host benötigt. Um die Anmeldedaten des SnapManager-Benutzerhosts im SnapManager-Benutzeranmeldungs-Cache zu speichern, legen Sie in der Datei smo.config die Eigenschaft Host.anmeldungs.persist auf true fest.

- Sie können den Benutzerzugriff auf das Repository autorisieren.
- Sie können den Benutzerzugriff auf Profile autorisieren.
- Sie können alle Benutzeranmeldeinformationen anzeigen.
- Sie können die Anmeldeinformationen eines Benutzers für alle Ressourcen (Hosts, Repositorys und Profile) löschen.
- Anmeldedaten für einzelne Ressourcen (Hosts, Repositorys und Profile) können gelöscht werden.

Verschlüsselte Passwörter für benutzerdefinierte Skripts speichern

Standardmäßig speichert SnapManager keine Hostanmeldeinformationen im Cache für Benutzeranmeldeinformationen. Sie können dies jedoch ändern. Sie können die Datei smo.config bearbeiten, um die Speicherung der Hostanmeldeinformationen zu ermöglichen.

Die Datei smo.config befindet sich unter <default Installation location>\Properties\smo.config

1. Bearbeiten Sie die Datei smo.config.
2. Legen Sie Host.Credentials.persist auf true fest.

Zugriffsberechtigung für das Repository

Mit SnapManager können Sie Anmeldedaten für Datenbankbenutzer für den Zugriff auf das Repository festlegen. Mithilfe von Zugangsdaten können Sie den Zugriff auf die SnapManager-Hosts, Repositorys, Profile und Datenbanken einschränken oder verhindern.

Wenn Sie die Anmeldeinformationen mithilfe des Befehls „Anmeldeinformationssatz“ festlegen, werden Sie von SnapManager nicht zur Eingabe eines Passworts aufgefordert.

Sie können Benutzeranmeldeinformationen festlegen, wenn Sie SnapManager oder höher installieren.

1. Geben Sie den folgenden Befehl ein:

   bbs-Anmeldeinformationssatz -Repository -dbname repo_Service_Name -Host repo_Host -Login -username repo_username [-password repo_password] -Port repo_Port

Zugriff auf Profile wird autorisiert

Mit SnapManager können Sie ein Kennwort für ein Profil festlegen, um unbefugten Zugriff zu verhindern.

1. Geben Sie den folgenden Befehl ein: smo Credential Set -profile -Name profile_Name [-password password]

Verwandte Informationen

Der Befehl Smo Credential Set

Anzeigen von Benutzeranmeldeinformationen

Sie können die Hosts, Profile und Repositorys auflisten, auf die Sie Zugriff haben.

1. Um die Ressourcen anzuzeigen, auf die Sie Zugriff haben, geben Sie diesen Befehl:Smo Anmeldeinformationsliste ein

Beispiel für die Anzeige von Benutzeranmeldeinformationen

In diesem Beispiel werden die Ressourcen angezeigt, auf die Sie Zugriff haben.

```
smo credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMOREPO/hotspur:1521
Host2_test_user@SMOREPO/hotspur:1521
user1_1@SMOREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]
Hosts:
Host2
Host5
```

Verwandte Informationen

Der Befehl smo Anmeldeinformationsliste

Löschen von Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile

Sie können den Cache Ihrer Anmeldeinformationen für Ressourcen (Hosts, Repositorys und Profile) löschen. Dadurch werden alle Ressourcen-Anmeldeinformationen für den Benutzer gelöscht, der den Befehl ausführt. Nach dem Löschen des Cache müssen Sie Ihre Anmeldeinformationen erneut authentifizieren, um auf diese gesicherten Ressourcen zugreifen zu können.

1. Um Ihre Anmeldeinformationen zu löschen, geben Sie den Befehl smo credentials clear in der SnapManager-CLI ein, oder wählen Sie in der SnapManager-Benutzeroberfläche **Admin** > **Anmeldeinformationen** > **Cache löschen** aus.
2. Schließen Sie die SnapManager-Benutzeroberfläche.

   HINWEIS:

   - Wenn Sie den Anmeldeinformationscache von der SnapManager-GUI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche nicht beenden.
   - Wenn Sie den Anmeldeinformationscache von der SnapManager-CLI gelöscht haben, müssen Sie die SnapManager-GUI neu starten.
   - Wenn Sie die verschlüsselte Anmeldedatei manuell gelöscht haben, müssen Sie die SnapManager-GUI erneut starten.
3. Um die Anmeldeinformationen erneut festzulegen, wiederholen Sie den Vorgang, um die Anmeldeinformationen für das Repository, den Profilhost und das Profil festzulegen. Weitere Informationen zum erneuten Einstellen der Benutzeranmeldeinformationen finden Sie unter „Anmeldeinformationen nach dem Löschen des Anmeldeinformationscache festlegen“.

Verwandte Informationen

Der Befehl smo Credential Clear

Einrichtung von Anmeldeinformationen nach Löschen des Anmeldeinformationscache

Nachdem Sie den Cache gelöscht haben, um die gespeicherten Benutzeranmeldeinformationen zu entfernen, können Sie die Anmeldeinformationen für die Hosts, Repositorys und Profile festlegen.

Sie müssen sicherstellen, dass Sie die gleichen Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil festlegen, das Sie zuvor angegeben haben. Beim Festlegen der Benutzeranmeldeinformationen wird eine verschlüsselte Anmeldedatei erstellt.

Die Anmeldeinformationen befinden sich unter C:\Dokumente und Einstellungen\Administrator\Applikationsdaten\NetApp\smo\3.3.0.

Führen Sie in der grafischen Benutzeroberfläche von SnapManager (GUI) die folgenden Schritte aus, wenn unter „Repositories“ kein Repository vorhanden ist:

1. Klicken Sie auf **Tasks** > **vorhandenes Repository hinzufügen**, um ein vorhandenes Repository hinzuzufügen.
2. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für das Repository festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf das Repository und wählen Sie **Öffnen**.
   b. Geben Sie im Fenster Repository Credentials Authentication die Benutzeranmeldeinformationen ein.
3. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für den Host festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf den Host unter dem Repository und wählen Sie **Öffnen**.
   b. Geben Sie im Fenster Host Credentials Authentication die Benutzeranmeldeinformationen ein.
4. Führen Sie die folgenden Schritte durch, um die Anmeldeinformationen für das Profil festzulegen:
   a. Klicken Sie mit der rechten Maustaste auf das Profil unter dem Host und wählen Sie **Öffnen**.
   b. Geben Sie im Fenster Authentifizierung für Profilanmeldeinformationen die Benutzeranmeldeinformationen ein.

Löschen von Anmeldeinformationen für einzelne Ressourcen

Sie können die Anmeldeinformationen für eine der gesicherten Ressourcen löschen, z. B. ein Profil, ein Repository oder einen Host. Auf diese Weise können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt die Anmeldeinformationen des Benutzers für alle Ressourcen zu löschen.

Verwandte Informationen

Der Befehl zum Löschen von Smo-Anmeldeinformationen

Benutzeranmeldeinformationen für Repositories werden gelöscht

Sie können die Anmeldeinformationen löschen, damit ein Benutzer nicht mehr auf ein bestimmtes Repository zugreifen kann. Mit diesem Befehl können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt die Anmeldeinformationen des Benutzers für alle Ressourcen zu löschen.

1. Um Repository-Anmeldeinformationen für einen Benutzer zu löschen, geben Sie diesen Befehl ein:smo

credit delete -Repository-dbnamerepo_Service_Name-hostrepo_Host-Login -usernamerepo_username -portrepo_Port

Löschen von Benutzeranmeldeinformationen für Hosts

Sie können die Anmeldeinformationen für einen Host löschen, sodass ein Benutzer nicht mehr darauf zugreifen kann. Mit diesem Befehl können Sie die Anmeldeinformationen nur für eine Ressource entfernen, anstatt alle Benutzeranmeldeinformationen für alle Ressourcen zu löschen.

1. Geben Sie zum Löschen der Hostanmeldeinformationen für einen Benutzer den folgenden Befehl ein:smo requeled -Host-nameHost_Name-username-username

Benutzeranmeldeinformationen für Profile werden gelöscht

Sie können die Benutzeranmeldeinformationen für ein Profil löschen, damit ein Benutzer nicht mehr darauf zugreifen kann.

1. Um die Profilanmeldeinformationen für einen Benutzer zu löschen, geben Sie den folgenden Befehl ein:smo requelm delete -profile-nameprofile_Name

Profilverwaltung für effiziente Backups

Sie müssen in SnapManager ein Profil für die Datenbank erstellen, auf der Sie einen Vorgang ausführen möchten. Sie müssen das Profil auswählen und dann den Vorgang auswählen, den Sie durchführen möchten.

Aufgaben im Zusammenhang mit Profilen

Sie können die folgenden Aufgaben ausführen:

- Erstellung von Profilen zur Aktivierung vollständiger oder partieller Backups und Backups auf primärem oder sekundärem Speicher

  Sie können auch Profile erstellen, um die Archiv-Log-Backups von den Backups der Datendatei zu trennen.

- Verifizieren von Profilen:
- Profile aktualisieren.
- Profile löschen.

Info zu Profilen und Authentifizierung

Wenn Sie ein Profil erstellen, können Sie eine Datenbank angeben und eine der folgenden Methoden zur Verbindung mit der Datenbank auswählen:

- Oracle-Authentifizierung mit Benutzername, Passwort und Port
- Betriebssystemauthentifizierung (OS) ohne Benutzername, Passwort oder Port

  Für die OS-Authentifizierung müssen Sie die Informationen für den OS-Kontobenutzer und -Gruppen

eingeben.

- Datenbank-Authentifizierung, wenn sqlnet.authentication_services auf „KEINE“ eingestellt ist. SnapManager verwendet dann für alle Verbindungen zur Zieldatenbank den Datenbankbenutzernamen und das Kennwort. SnapManager kann auch die native Windows-Authentifizierung verwenden, wenn sqlnet.authentication_services auf NTS eingestellt ist.

Sie können sqlnet.authentication_services auf NONE nur in den folgenden Umgebungen einstellen:

Datenbank-Layout	Oracle Version	Wird die Datenbankauthentifizierung für die Zieldatenbank unterstützt
Alle nicht-ASM- und nicht-RAC-Datenbanken	Oracle 10g und Oracle 11g (weniger als 11.2.0.3)	Ja.

Hinweis: Nachdem Sie sqlnet.authentication_services deaktiviert haben und die Authentifizierungsmethode in die Datenbankauthentifizierung ändern, müssen Sie sqlnet.authentication_services auf KEINE einstellen.

Wenn Sie zum ersten Mal auf ein Profil zugreifen, müssen Sie Ihr Profilkennwort eingeben. Nachdem Sie Ihre Anmeldedaten eingegeben haben, können Sie die Datenbank-Backups im Profil anzeigen.

Verwandte Informationen

Welche Profile sind

Profile werden erstellt

Beim Erstellen von Profilen können Sie dem Profil ein bestimmtes Oracle-Datenbankbenutzerkonto zuweisen. Sie können die Aufbewahrungsrichtlinie für das Profil festlegen und die Anzahl und Dauer der Aufbewahrung für jede Aufbewahrungsklasse festlegen.

Wenn Sie die Werte der Parameter -Login, -password und -Port der Datenbank nicht angeben, verwendet der Authentifizierungsmodus des Betriebssystems die Standardanmeldeinformationen.

Während der Erstellung eines Profils führt SnapManager eine Überprüfung der Berechtigung zur Wiederherstellung durch, um den Wiederherstellungsmechanismus zu bestimmen, mit dem die Datenbank wiederhergestellt werden kann.

Mit SnapManager (3.2 oder höher) können Sie Archivprotokolldateien von den Datendateien trennen, während Sie ein neues Profil erstellen oder ein vorhandenes Profil aktualisieren. Nachdem Sie die Sicherung mit dem Profil getrennt haben, können Sie entweder nur die Datendateien-only-Backup oder Archiv-Log-only-Backup der Datenbank erstellen. Sie können das neue Profil oder das aktualisierte Profil verwenden, um das Backup zu erstellen, das sowohl die Datendateien als auch die Archivprotokolldateien enthält. Sie können das Profil jedoch nicht zum Erstellen der vollständigen Sicherung oder zum Zurücksetzen der Einstellungen verwenden.

Profile zur Erstellung vollständiger und partieller Backups

Sie können Profile erstellen, um das vollständige Datenbank-Backup mit den Datendateien, Kontrolldateien, Archivprotokolldateien und partiellen Datenbank-Backups zu erstellen, die bestimmte Datendateien oder Tablespaces enthalten, alle Kontrolldateien und alle Archivprotokolldateien. SnapManager erlaubt Ihnen nicht, mithilfe der Profile, die für vollständige und teilweise Backups erstellt wurden, separate Archiv-Log-Backups zu

erstellen.

Profile zur Erstellung von nur-Datendateien-Backups und nur archivalogs-Backups

Wenn Sie ein neues Profil erstellen, können Sie -separatem-archivlog-Backups einbeziehen und das Archiv-Log-Backup von der Datendatei-Sicherung trennen. Sie können das vorhandene Profil auch aktualisieren, um die Sicherung des Archivprotokolls von der Datensicherung der Datendatei zu trennen.

Mithilfe der neuen Profiloptionen können Sie die Backups des Archivprotokolls trennen und folgende SnapManager-Vorgänge durchführen:

- Erstellen Sie eine Backup-Datei für Archivprotokolle
- Löschen Sie eine Sicherung des Archivprotokolls
- Mounten Sie ein Backup für das Archivprotokoll
- Kostenlose Backup eines Archivprotokolls

Während das Profil erstellt wird, um Archiv-Log-Backups von der Datensicherung zu trennen, wenn die Archiv-Log-Dateien nicht in der Datenbank vorhanden sind, für die das Profil erstellt wird, dann ist eine Warnung Archived Log-Datei nicht im aktiven Dateisystem vorhanden. Die Versionen der archivierten Protokolldatei, die früher als die Version des <Archiv-Log-Threads> -Protokolls waren, werden nicht in die Sicherung aufgenommen. Selbst wenn Sie Backups für diese Datenbank erstellen, sind die Archiv-Log-Dateien in den Datenbank-Backups nicht verfügbar.

Wenn beim Erstellen eines Profils ein Fehler auftritt, verwenden Sie den Befehl „Smosystem dump“. Nachdem Sie ein Profil erstellt haben, verwenden Sie die Befehle Smooperation dump und smoprofile dump, wenn Sie einen Fehler haben.

1. Um ein Profil mit einem Benutzernamen, Kennwort und Port (Oracle-Authentifizierung) zu erstellen, geben Sie den folgenden Befehl ein: bbs-Profile create -profileprofil [-profile-passwordprofile_password] -Repository-dbnamerepo_dbname-hostrepo_Host-portrepo_Port-Login-usernamerepo_username -Database-dbnamepo_addbnamens2 [-Login] { [-commentation-adressem {] [-incountname} }-adressem] [-adressem] [-adressed-adressem] [-adressem] [-adressem] [-adressem] [-adressem] [-adressem] [-adressem] [-adressem] [-adressem] [-concement-adressed-adressem] [-adressem] [-adressed-adressem] [-adressed-adressem] [-adressem] [-adressed-adressem] [-adressed-convertninto] [-adressem] [-adressem] [-adressed

   Weitere Optionen für diesen Befehl:

   [-Force] [-noprompt]

   Je nach Zugriffsart auf die Datenbank können Sie auch weitere Optionen bei der Erstellung von Profilen berücksichtigen.

Wenn…	Dann…
Sie möchten die Datenbankauthentifizierung verwenden, um ein Profil zu erstellen	Geben Sie die Anmeldedaten für die Datenbank an.

Sie wollen eine Backup Retention Policy für Backups angeben	Geben Sie entweder den Aufbewahrungszähler oder die Dauer für eine Aufbewahrungsklasse oder beides an. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). • -Hourly ist die stündliche Aufbewahrungsklasse, für die [-count n] [-duration m] der Aufbewahrungszähler und die Aufbewahrungsdauer sind, bzw.. • -Daily ist die tägliche Aufbewahrungsklasse, für die [-count n] [-durationm] die Aufbewahrungszahl und Aufbewahrungsdauer sind, bzw.. • -Weekly ist die wöchentliche Aufbewahrungsklasse, für die [-count n] [-duration m] der Aufbewahrungszähler und die Aufbewahrungsdauer sind, bzw.. • -Monthly ist die monatliche Aufbewahrungsklasse, für die [-count n] [-durationm] der Aufbewahrungszähler und die Aufbewahrungsdauer sind, bzw..

Sie möchten die E-Mail-Benachrichtigung für den Abschlussstatus der Datenbankvorgänge aktivieren	Geben Sie die folgenden Optionen und Variablen an: • -Summary-notification ermöglicht Ihnen die Konfiguration einer E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank. • -Notification ermöglicht Ihnen, eine E-Mail-Benachrichtigung über den Status des Datenbankvorgangs für ein Profil zu erhalten. • -Success-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung über den erfolgreichen Datenbankvorgang zu erhalten, der mit einem neuen oder vorhandenen Profil durchgeführt wird. • -Failure-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung über den fehlgeschlagenen Datenbankvorgang zu erhalten, der mit einem neuen oder vorhandenen Profil durchgeführt wird. • -Subjectsubject_Text gibt den Subjekttext für die E-Mail-Benachrichtigung an, während ein neues Profil oder ein vorhandenes Profil erstellt wird. Wenn die Benachrichtigungseinstellungen nicht für das Repository konfiguriert sind und Sie versuchen, mithilfe der CLI Profil- oder Übersichtsbenachrichtigungen zu konfigurieren, wird die folgende Meldung im Konsole-Protokoll protokolliert: SMO-14577: Benachrichtigungseinstellungen nicht konfiguriert. Wenn Sie die Benachrichtigungseinstellungen konfiguriert haben und versuchen, eine zusammenfassende Benachrichtigung mithilfe der CLI zu konfigurieren, ohne eine zusammenfassende Benachrichtigung für das Repository zu aktivieren, wird die folgende Meldung im Konsole-Protokoll angezeigt: SMO-14575: Konfiguration der zusammenfassenden Benachrichtigung für dieses Repository nicht verfügbar_

Sie wollen Archivprotokolldateien getrennt von Datendateien sichern	Geben Sie die folgenden Optionen und Variablen an: • -Separate-archivlog-Backups ermöglicht es Ihnen, das Archiv-Log-Backup vom Datendatei-Backup zu trennen. • -Retention-archivlog-Backups legt die Aufbewahrungsdauer für Archiv-Log-Backups fest. Sie müssen eine positive Aufbewahrungsdauer angeben. Die Backups für das Archivprotokoll werden basierend auf der Aufbewahrungsdauer des Archivprotokolls aufbewahrt. Die Backups der Datendateien werden gemäß den bestehenden Aufbewahrungsrichtlinien beibehalten. • -Include-with-Online-Backups beinhalten das Archiv-Log-Backup zusammen mit dem Online-Datenbank-Backup. Mit dieser Option können Sie ein Backup- und Archivprotokoll für Online-Datendateien zum Klonen erstellen. Wenn diese Option eingestellt ist, werden bei jeder Erstellung eines Backups von Online-Datendateien die Archiv-Logs-Backups zusammen mit den Datendateien sofort erstellt. • -No-include-with-Online-Backups beinhalten nicht das Archiv-Log-Backup zusammen mit dem Datenbank-Backup.
Nach der erfolgreichen Profilerfassungsoperation können Sie die Dump-Dateien sammeln	Geben Sie die -dump-Option am Ende des Befehls zum Erstellen von Profilen an.

Verwandte Informationen

So sammeln Sie Speicherauszugsdateien

Benennen von Snapshot-Kopien

Sie können eine Namenskonvention oder ein Muster angeben, um die Snapshot Kopien in Bezug auf das Profil zu beschreiben, das Sie erstellen oder aktualisieren. Sie können auch benutzerdefinierten Text in alle Namen von Snapshot Kopien einfügen.

Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster wird nur für Snapshot Kopien angewendet, die noch nicht aufgetreten sind. Snapshot Kopien, die vorhanden sind und das frühere Snapshot-Namensmuster behalten.

In den folgenden Beispielen werden die beiden Namen von Snapshot Kopien aufgeführt, die für ein Volume erstellt wurden. Die zweite aufgeführte Snapshot Kopie befindet sich mitten in seinem Namen *F_H_1*. Die „1“ gibt an, dass es die erste Snapshot-Kopie ist, die im Backup-Satz erstellt wurde. Die erste aufgeführte Snapshot Kopie ist der neueste und verfügt über eine „2“. Dies bedeutet, dass es sich um die zweite erstellte Snapshot Kopie handelt. Die „1“ Snapshot Kopie enthält die Datendateien; die Snapshot Kopie „2“ enthält die Kontrolldateien. Da nach der Snapshot Kopie der Datendatei Snapshot Kopien der Kontrolldatei Snapshot Kopien erstellt werden müssen, sind zwei Snapshot Kopien erforderlich.

```
smo_profile_sid_f_h_2_8ae482831ad14311011ad14328b80001_0
smo_profile_sid_f_h_1_8ae482831ad14311011ad14328b80001_0
```

Das Standardmuster enthält das erforderliche smid, wie im Folgenden dargestellt:

- Standardmuster: smo_{Profile}_{db-sid}_{Scope}_{Mode}_{smid}
- Beispiel: smo_my_Profile_rac51_f_h_2_8abc01e915a55ac50115a55acc8d0001_0

Im Namen der Snapshot Kopie können Sie die folgenden Variablen verwenden:

Variablenname	Beschreibung	Beispielwert
smid (erforderlich)	Die eindeutige SnapManager-ID ist das einzige erforderliche Element, wenn ein Name für die Snapshot Kopie erstellt wird. Mit dieser ID wird sichergestellt, dass Sie einen eindeutigen Snapshot-Namen erstellen.	8abc01e915a55ac50115a55acc8d0001_0
Klasse (optional)	Aufbewahrungsklasse im Zusammenhang mit dem Backup für das Profil und angezeigt durch Stunden (h), täglich (d), wöchentlich (w), monatlich (m) oder unbegrenzt (U).	d
Kommentar (optional)	Kommentar zum Backup für das Profil. Leerzeichen in diesem Feld werden in Unterstriche konvertiert, wenn der Name der Snapshot Kopie abgeschlossen ist.	Sample_comment_Spaces_ersetzte
Datum (optional)	Datum, an dem das Backup für das Profil durchgeführt wird. Datumswerte werden bei Bedarf mit Nullen aufgefüllt. (jjjjmmtt)	20070218
db-Host (optional)	Datenbank-Host-Name, der dem Profil zugeordnet ist, das erstellt oder aktualisiert wird.	Mein_Host

db-Name (optional)	Dem von Ihnen erstellten Snapshot-Kopie zugeordneten Datenbanknamen.	rac5
db-sid (optional)	Der von Ihnen erstellten Snapshot Kopie zugeordnete Datenbank-sid.	Renn51
Beschriftung (optional)	Mit der Sicherung für das Profil verknüpfte Bezeichnung.	Sample_Label
Modus (optional)	Gibt an, ob die Sicherung online (h) oder offline (c) abgeschlossen ist.	H
Profil (optional)	Profilname, der dem von Ihnen erstellten Backup zugeordnet ist.	My_Profile
Umfang (optional)	Gibt an, ob das Backup entweder voll (f) oder partiell (p) ist.	f
Zeit (optional)	Die Dauer des Backups für das Profil. Zeitwerte für diese Variable Verwenden Sie die 24-Stunden-Uhr und werden bei Bedarf mit Nullen gepolstert. Beispielsweise werden 5:32 und 8 Sekunden als 053208 (hhhmmss) angezeigt.	170530
Zeitzone (optional)	Für den Ziel-Datenbank-Host angegebene Zeitzone.	GESCHÄTZT
Benutzertext (optional)	Benutzerdefinierter Text, den Sie eingeben können.	Prod

Hinweis: SnapManager für Oracle unterstützt das Doppelpunkt (:) Symbol in den langen Formen der Namen für Snapshot Kopien nicht.

Profile werden umbenannt

Mit SnapManager können Sie das Profil umbenennen, wenn Sie das Profil aktualisieren. Die SnapManager Funktionen, die in dem Profil festgelegt werden, sowie die vor der Umbenennung durchzuführenden Vorgänge werden, werden für das umbenannte Profil beibehalten.

- Sie müssen sicherstellen, dass während der Umbenennung des Profils keine SnapManager-Vorgänge auf dem Profil ausgeführt werden.

Sie können das Profil sowohl von der SnapManager Befehlszeilenschnittstelle (CLI) als auch von der grafischen Benutzeroberfläche (GUI) umbenennen. Bei der Aktualisierung des Profils überprüft und aktualisiert SnapManager den Profilnamen im Repository.

SnapManager unterstützt das Umbenennen des Profils im Fenster Multi-Profile-Update nicht.

Wenn Sie einen neuen Profilnamen angeben, wird der neue Profilname im Client-seitigen Anmeldeinformationcache hinzugefügt und der frühere Profilname wird entfernt. Wenn Sie das Profil von einem Client umbenennen, wird der Anmeldeinformationscache nur von diesem Client aktualisiert. Sie müssen den Befehl smoprofile SYNC von jedem der Clients ausführen, um den neuen Anmeldeinformationscache mit dem neuen Profilnamen zu aktualisieren.

Sie können das Passwort für das Profil mithilfe des Befehls smo Credential Set festlegen.

Wenn der Profilname in einem Benennungsmuster für die Snapshot Kopie enthalten war, wird beim Umbenennen eines Profils der neue Name für das Profil aktualisiert. Alle SnapManager-Vorgänge, die im Profil ausgeführt werden, verwenden den neuen Profilnamen. Die mit einem früheren Profil erstellten Backups besitzen weiterhin den früheren Profilnamen und werden zur Durchführung anderer SnapManager Vorgänge verwendet.

Wenn Sie ein Rolling Upgrade für SnapManager-Server-Hosts durchführen, müssen Sie sicherstellen, dass Sie das gesamte Upgrade durchführen, bevor Sie das Profil umbenennen.

Der neue Name für das Profil wird nur von dem SnapManager-Client aktualisiert, aus dem die Anforderung stammt. Die SnapManager-Clients, die mit dem SnapManager-Server verbunden sind, werden nicht über die Änderung des Profilnamens benachrichtigt. Sie können das Betriebsprotokoll überprüfen, um über die Änderung des Profilnamens zu informieren.

Wenn ein geplanter Backup-Vorgang zum Zeitpunkt der Umbenennung des Profils beginnt, schlägt der geplante Vorgang fehl.

1. Geben Sie den folgenden Befehl ein: smo Profilupdate -profilprofil [-New-profilenew_profile_Name]

Profilkennwörter werden geändert

Um die vorhandenen Profile im Repository zu schützen, sollten Sie die Passwörter für die Profile aktualisieren. Sie können dieses aktualisierte Passwort anwenden, wenn Sie ein Backup mit diesem Profil erstellen.

1. Um das Profilpasswort für ein vorhandenes Profil zu aktualisieren, geben Sie den folgenden Befehl ein:

   smo Profile Update -profile_Name -profile-password

Verwandte Informationen

Der Befehl smoprofile Update

Profilkennwort wird zurückgesetzt

Sie können das Profilkennwort zurücksetzen, wenn Sie sich nicht an das Passwort erinnern, das Sie beim Erstellen des Profils angegeben haben.

- Sie müssen sicherstellen, dass der SnapManager-Server auf der Repository-Datenbank ausgeführt wird.
- Sie müssen über die lokalen Administratoranmeldedaten des Hosts verfügen, auf dem sich die Repository-Datenbank befindet.

- Sie müssen sicherstellen, dass das Profil nicht für einen Vorgang verwendet wird, wenn das Passwort für dieses Profil zurückgesetzt wird.

Sie können das Passwort entweder von der SnapManager-CLI oder von der GUI aus zurücksetzen. Beim Zurücksetzen des Passworts fragt SnapManager den SnapManager-Server auf dem Repository-Host ab, um das Betriebssystem für den Repository-Host zu identifizieren. Sie müssen die Anmeldeinformationen für den autorisierten Benutzer für die Verbindung zum Repository-Host eingeben. Der SnapManager-Server authentifiziert Benutzer mit ihren lokalen Administratoranmeldeinformationen auf der Repository-Datenbank. Wenn die Authentifizierung erfolgreich ist, setzt SnapManager das Profilkennwort auf dem SnapManager-Server mit dem neuen Passwort zurück.

SnapManager führt den Verlauf der Vorgänge zum Zurücksetzen von Passwörtern nicht aus.

1. Zurücksetzen des Profilpassworts durch Eingabe des folgenden Befehls: smo password Reset -profilprofile [-profile-passwordprofile_password] [-Repository-hostadmin-passwordadmin_password]

Zugriff auf Profile wird autorisiert

Mit SnapManager können Sie ein Kennwort für ein Profil festlegen, um unbefugten Zugriff zu verhindern.

1. Geben Sie den folgenden Befehl ein: smo Credential Set -profile -Name profile_Name [-password password]

Verwandte Informationen

Der Befehl Smo Credential Set

Profile werden überprüft

Sie können überprüfen, ob ein vorhandenes Profil korrekt eingerichtet wurde. Wenn Sie ein Profil überprüfen, überprüft SnapManager die Umgebung auf das von Ihnen angegebene Profil und überprüft, ob das Profil eingerichtet ist und auf die Datenbank in diesem Profil zugegriffen werden kann.

1. Um zu überprüfen, ob das Profil ordnungsgemäß eingerichtet ist, geben Sie folgenden Befehl ein: smo profile verify -profile_Name

Verwandte Informationen

Der Befehl smoprofile verify

Profile werden aktualisiert

Sie können die Profile aktualisieren, um das Profilkennwort, die Anzahl der zu behaltenden Backups, den Zugriff auf die Datenbank, die Betriebssystemauthentifizierung (OS) auf die Datenbankauthentifizierung und umgekehrt sowie Informationen zum Host zu ändern. Wenn sich die Kennwortinformationen der Oracle-Datenbank ändern, müssen Sie diese Informationen auch im Profil ändern.

Mit SnapManager (3.2 oder höher) können Sie das Profil aktualisieren und die Archiv-Log-Backups von den

Datensicherungen der Datendatei trennen, indem Sie die Option -separatem-archivlog-Backups verwenden. Sie können eine separate Aufbewahrungsdauer für das Backup des Archivprotokolls festlegen. Mit SnapManager können Sie das Archivprotokoll-Backup zusammen mit dem Online-Datenbank-Backup einbeziehen. Außerdem können Sie zum Klonen eine Online-Datendatei-Backup- und ein Archivprotokoll-Backup erstellen. Wenn Sie eine Sicherung von Online-Datendateien erstellen, werden die Archivprotokolle sofort zusammen mit den Datendateien erstellt.

1. Geben Sie den folgenden Befehl ein: bbs-Profil-Update -profilprofil [-New-profilenew_profile_Name] [-profile-passwordprofile_password][-Database-dbnaedb_dbname-Host db_Host [-siddb_sid] [-Login-usernamedb_username-address2] [-rman{{ {}}}-controduct_adressem [-] [-] [-commentailtmnem_commend] [-[-] [-] [-] [-]]] [-]] [-]]] [-commodmprotodmnesson-[-] [-commend_commendnesson-[-[-] [-] [-] [-] [-] [-]] [-]] [-]] [-]]]] [-commendmnesson-] [-commendmprompromptpromnesson-commendness2] [-[-] [-] [-] [-] [-] [

   Weitere Optionen für diesen Befehl:

   [-Force] [-noprompt]

Ihr Ziel ist	Dann…
Ändern Sie die Backup Retention Policy für Backups der Datenbank im Profil	Geben Sie entweder den Aufbewahrungszeitraum oder die Aufbewahrungsdauer für eine Aufbewahrungsklasse oder beides an, um die Aufbewahrungsrichtlinie zu ändern. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). • -Hourly ist die stündliche Aufbewahrungsklasse, für die [-countn] [-durationm]]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw.. • -Daily ist die tägliche Aufbewahrungsklasse, für die [-countn] [-durationm]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw.. • -Weekly ist die wöchentliche Aufbewahrungsklasse, für die [-countn] [-durationm]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw.. • -Monthly ist die monatliche Aufbewahrungsklasse, für die [-countn] [-durationm]]] die Aufbewahrungszahl und die Aufbewahrungsdauer sind, bzw..

E-Mail-Benachrichtigungen für den Abschlussstatus der Datenbankvorgänge aktivieren	Geben Sie die folgenden Optionen und Variablen an: • -Summary-notification ermöglicht Ihnen die Konfiguration einer E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank. • -Notification ermöglicht Ihnen, eine E-Mail-Benachrichtigung über den Status des Datenbankvorgangs für ein Profil zu erhalten. • -Success-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung nach Abschluss eines erfolgreichen Datenbankvorgangs zu erhalten, der mit einem neuen oder einem vorhandenen Profil durchgeführt wird. • -Failure-emailemail_address2 ermöglicht es Ihnen, eine E-Mail-Benachrichtigung über einen fehlgeschlagenen Datenbankvorgang zu erhalten, der mit einem neuen oder einem vorhandenen Profil durchgeführt wird. • -Subjectsubject_Text gibt den Subjekttext für die E-Mail-Benachrichtigung an, während ein neues Profil oder ein vorhandenes Profil erstellt wird. Wenn die Benachrichtigungseinstellungen nicht für das Repository konfiguriert sind und Sie versuchen, Profile- oder Übersichtsbenachrichtigungen mithilfe der Befehlszeilenschnittstelle (CLI) zu konfigurieren, wird die folgende Meldung im Konsolenprotokoll protokolliert: SMO-14577: Benachrichtigungseinstellungen nicht konfiguriert. Wenn Sie die Benachrichtigungseinstellungen konfiguriert haben und versuchen, eine zusammenfassende Benachrichtigung mithilfe der CLI zu konfigurieren, ohne dass eine zusammenfassende Benachrichtigung für das Repository aktiviert wird, wird die folgende Meldung im Konsole-Protokoll protokolliert: SMO-14575: Konfiguration der zusammenfassenden Benachrichtigung für dieses Repository nicht verfügbar

Aktualisieren Sie das Profil, um eine Sicherung der Archiv-Log-Dateien separat zu erstellen	Geben Sie die folgenden Optionen und Variablen an: • -Separate-archivlog-Backups ermöglicht es Ihnen, eine Sicherung der Archivprotokolldateien getrennt von den Datenbankdateien zu erstellen. Nachdem Sie diese Option angegeben haben, können Sie entweder ein Datendatei-only Backup oder ein Backup nur mit Archivdateien erstellen. Sie können keine vollständige Sicherung erstellen. Außerdem können Sie die Profileinstellungen nicht durch Trennen der Sicherung zurücksetzen. SnapManager behält die Backups auf Basis der Aufbewahrungsrichtlinie für die Backups bei, die vor der Erstellung eines rein archivorientierten Backups erstellt wurden. • -Retention-archivlog-Backups legt die Aufbewahrungsdauer für Archiv-Log-Backups fest. Wenn Sie das Profil zum ersten Mal aktualisieren, können Sie die Archiv-Log-Backups vom Datendatei-Backup mit der Option -separatem-archivlog -Backups trennen; Sie müssen die Aufbewahrungsdauer für die Archiv-Log-Backups mit der Option -restyle-archivelog -Backups angeben. Die Einstellung der Aufbewahrungsdauer ist optional, wenn Sie das Profil später aktualisieren. • -Include-with-Online-Backups geben an, dass das Archiv-Log-Backup zusammen mit dem Datenbank-Backup enthalten ist. • -No-include-with-Online-Backups gibt an, dass die Sicherung der Archivprotokolldatei nicht zusammen mit der Datenbank-Sicherung enthalten ist.
Ändern Sie den Hostnamen der Zieldatenbank	Geben Sie -hostNew_db_Host an, um den Hostnamen des Profils zu ändern.

Sammeln Sie die Dump-Dateien nach dem Profil-Update-Vorgang	Geben Sie die Option -dump an.

2. Geben Sie zum Anzeigen des aktualisierten Profils den folgenden Befehl ein: smo Profile show

Verwandte Informationen

So sammeln Sie Speicherauszugsdateien

Profile werden gelöscht

Sie können ein Profil jederzeit löschen, solange es keine erfolgreichen oder unvollständigen Backups enthält. Sie können Profile löschen, die freigegebene oder gelöschte Backups enthalten.

1. Um ein Profil zu löschen, geben Sie den folgenden Befehl ein:smo profile delete -profile profile profile_Name

Verwandte Informationen

Der Befehl smoprofile delete

Backup von Datenbanken

SnapManager ermöglicht das Backup von Daten in lokalen Storage-Ressourcen mithilfe von Post-Processing-Skripten.

SnapManager bietet folgende Optionen zum Sichern, Wiederherstellen und Wiederherstellen der Daten in Ihrer Datenbank:

- Sichern Sie die gesamte Datenbank oder einen Teil davon.

  Wenn Sie einen Teil davon sichern, geben Sie eine Gruppe von Tabellen oder eine Gruppe von Datendateien an.

- Sichern Sie die Datendateien und archivieren Sie Log-Dateien separat.
- Erstellen Sie ein Backup von Datenbanken im primären Storage (auch als lokaler Storage bezeichnet) und sichern Sie sie, indem Sie diese mithilfe von Nachbearbeitungsskripten auf sekundäre Speicherressourcen sichern.
- Planen Sie routinemäßige Backups.

Wie sich SnapManager (3.2 oder höher) von früheren SnapManager Versionen unterscheidet

SnapManager (3.1 oder älter) ermöglicht Ihnen die Erstellung vollständiger Datenbank-Backups, die Datendateien, Kontrolldateien und Archivprotokolldateien enthalten.

SnapManager (3.1 oder älter) verwaltet nur die Datendateien. Die Archivprotokolldateien werden mithilfe von Lösungen außerhalb von SnapManager aufbewahrt.

SnapManager (3.1 oder früher) hat die folgenden Einschränkungen beim Management von Datenbank-Backups:

- Performance-Einbußen

  Wenn Sie ein vollständiges Online-Datenbank-Backup durchführen (wenn sich die Datenbank im Backup-Modus befindet), reduziert sich die Performance der Datenbank für den Zeitraum, bis das Backup erstellt wird. In SnapManager (ab 3.2) können begrenzte Datenbank-Backups und häufige Archiv-Log-Backups erstellt werden. Durch häufige Backups für Archivprotokolle kann verhindert werden, dass die Datenbank im Backup-Modus platziert wird.

- Manuelle Wiederherstellung und Wiederherstellung

  Wenn die erforderlichen Archivprotokolldateien nicht im aktiven Dateisystem vorhanden sind, müssen Datenbankadministratoren erkennen, welches Backup die Archivprotokolldateien enthält, die Datenbank-Backups mounten und die wiederhergestellte Datenbank wiederherstellen. Dieser Prozess ist zeitaufwändig.

- Platzbeschränkungen

  Wenn ein Datenbankbackup erstellt wird, werden die Ziele für das Archivprotokoll voll, sodass die Datenbank nicht reagiert, bis ausreichend Speicherplatz auf dem Speicher erstellt wird. In SnapManager (3.2 oder höher) können die Archiv-Log-Dateien aus dem aktiven Dateisystem heraus geschnitten werden, um regelmäßig Speicherplatz freizugeben.

Warum Archiv-Log-Backups wichtig sind

Archivprotokolldateien sind erforderlich, um die Datenbank nach einer Wiederherstellung vorwärts zu verschieben. Jede Transaktion auf einer Oracle-Datenbank wird in den Archiv-Log-Dateien erfasst (wenn sich die Datenbank im Archiv-Log-Modus befindet). Datenbankadministratoren können die Datenbank-Backups mithilfe der Archivprotokolldateien wiederherstellen.

Vorteile von nur-archivlog Backups

- Separate Aufbewahrungsdauer für nur archivlog Backups

  Es kann weniger Aufbewahrungsdauer für die rein archivbasierten Backups haben, die für die Wiederherstellung erforderlich sind.

- Schützt die nur archivlog Backups mit Nachverarbeitungsskripten
- Verbessert die Performance der Datenbank
- Konsolidiert Backups für Archivprotokolle

  SnapManager konsolidiert die Archiv-Protokoll-Backups jedes Mal, wenn Sie ein Backup erstellen, indem die doppelten Archiv-Log-Backups freigegeben werden.

Welche SnapManager Datenbank-Backups sind

SnapManager ermöglicht Ihnen die Durchführung verschiedener Backup-Aufgaben. Sie können Aufbewahrungsklassen zuweisen, um festzulegen, wie lange das Backup aufbewahrt werden kann. Sobald diese Frist erreicht ist, wird das Backup gelöscht.

- Erstellen von Backups auf dem primären Storage
- Erstellen Sie mit Nachbearbeitungsskripten geschützte Backups auf den sekundären Storage-Ressourcen

- Überprüfen Sie, ob die Backups erfolgreich abgeschlossen wurden
- Zeigen Sie eine Liste von Backups an
- Planen Sie Backups über die grafische Benutzeroberfläche
- Verwalten Sie die Anzahl der beibehaltenen Backups
- Kostenlose Backup-Ressourcen
- Mounten und unmounten Sie Backups
- Backups löschen

SnapManager erstellt Backups mithilfe einer der folgenden Aufbewahrungsklassen:

- Stündlich
- Täglich
- Wöchentlich
- Monatlich
- Unbegrenzt

Wenn neue Datendateien zur Datenbank hinzugefügt werden, sollten Sie sofort eine neue Sicherung erstellen. Wenn Sie außerdem ein Backup wiederherstellen, das vor dem Hinzufügen der neuen Datendateien erstellt wurde, und versuchen Sie, es nach dem Hinzufügen der neuen Datendateien zu einem Punkt wiederherzustellen, kann der automatische Recovery-Prozess fehlschlagen. Weitere Informationen zum Prozess zur Wiederherstellung der nach einem Backup hinzugefügten Datendateien finden Sie in der Oracle-Dokumentation.

Welche vollständigen und teilweisen Backups sind

Sie können ein Backup der gesamten Datenbank oder nur eines Teils davon erstellen. Wenn Sie einen Teil der Datenbank sichern möchten, können Sie wahlweise eine Gruppe von Tabellen oder Datendateien sichern. Sie können dabei ein separates Backup sowohl von Tabellen als auch Datendateien durchführen.

In der folgenden Tabelle sind die Vorteile und Folgen der einzelnen Backup-Typen aufgeführt:

Backup-Typ	Vorteile	Nachteile
Voll	Minimiert die Anzahl der Snapshot Kopien. Bei Online-Backups befindet sich jede Tablespace für die gesamte Zeit des Backup-Vorgangs im Backup-Modus. SnapManager erstellt für jedes Volume, das die Datenbank verwendet, eine Snapshot-Kopie sowie eine Snapshot-Kopie jedes Volumes, die sich die Protokolldateien befinden.	Bei Online-Backups befindet sich jede Tablespace für die gesamte Zeit des Backup-Vorgangs im Backup-Modus.

Teilweise	Minimiert die Zeitdauer, die jeder Tablespace im Backup-Modus verbringt. SnapManager gruppiert die von Tablespaces erstellten Snapshot Kopien. Jede Tablespace befindet sich im Backup-Modus nur lang genug, um die Snapshot-Kopien zu erstellen. Diese Methode zur Gruppierung der Snapshot Kopien minimiert die Schreibvorgänge in physischen Blöcken in Protokolldateien während eines Online-Backups.	Das Backup kann das Erstellen von Snapshot Kopien mehrerer Tabellen im selben Volume erfordern. Diese Methode kann dazu führen, dass SnapManager während des Backups mehrere Snapshot Kopien eines einzelnen Volumes erstellt.

Hinweis: Obwohl Sie eine partielle Sicherung durchführen können, müssen Sie immer eine vollständige Sicherung der gesamten Datenbank durchführen.

Backup-Typen und die Anzahl der Snapshot Kopien

Der Backup-Typ (vollständig oder teilweise) beeinflusst die Anzahl der Snapshot-Kopien, die SnapManager erstellt. Für eine vollständige Sicherung erstellt SnapManager eine Snapshot Kopie jedes Volumes, während für ein partielles Backup SnapManager eine Snapshot Kopie jeder Tablespaces-Datei erstellt.

Data ONTAP begrenzt die maximale Anzahl an Snapshot Kopien auf 255 pro Volume. Diese maximale Anzahl erreichen Sie möglicherweise nur, wenn Sie SnapManager für eine große Anzahl von Backups konfigurieren, bei denen jedes Backup aus mehreren Snapshot Kopien besteht.

Um einen ausreichenden Backup-Pool verfügbar zu halten und gleichzeitig sicherzustellen, dass das maximale Limit von Snapshot Kopien pro Volume nicht erreicht wird, müssen Sie Backups entfernen, wenn sie nicht mehr benötigt werden. Sie können die SnapManager Aufbewahrungsrichtlinie so konfigurieren, dass erfolgreiche Backups entfernt werden, nachdem ein bestimmter Schwellenwert für eine bestimmte Backup-Frequenz erreicht wurde. Nachdem SnapManager beispielsweise vier erfolgreiche tägliche Backups erstellt hat, entfernt SnapManager die täglich erstellten Backups am Vortag.

In den folgenden Tabellen wird gezeigt, wie SnapManager Snapshot Kopien auf Grundlage des Backup-Typs erstellt. Das Beispiel in der Tabelle geht davon aus, dass Datenbank-Z zwei Volumes umfasst, jedes Volume zwei Tabellen (TS1 und TS2) und jeder Tablespace zwei Datenbankdateien (ts1_1.dbf, ts1_2.dbf, ts2_1.dbf und ts2_2.dbf) umfasst.

In diesen Tabellen wird gezeigt, wie die beiden Backup-Typen verschiedene Anzahl von Snapshot Kopien erstellen.

SnapManager erstellt Snapshot Kopien auf Volume-Ebene anstelle von Tablespaces, die in der Regel die Anzahl der zu erstellenden Snapshot Kopien verringern.

Beide Backups erstellen auch Snapshot Kopien der Log-Dateien.

Volumes in Datenbank	Tablespace TS1 (enthält 2 Datenbankdateien)	Tablespace TS2 (enthält 2 Datenbankdateien)	Snapshot Kopien werden erstellt	Gesamtzahl der Snapshot Kopien
E:\Daten	TS1_1.dbf	TS2_1.dbf	1 pro Volume	2

Volumes in Datenbank	Tablespace TS1 (enthält 2 Datenbankdateien)	Tablespace TS2 (enthält 2 Datenbankdateien)	Snapshot Kopien werden erstellt	Gesamtzahl der Snapshot Kopien
E:\Daten	TS1_1.dbf	TS2_1.dbf	2 pro Datei	4

Vollständige Online-Backups

Während eines vollständigen Online-Backups sichert SnapManager die gesamte Datenbank und erstellt Snapshot-Kopien auf Volume-Ebene (nicht auf Ebene der Tablespaces).

SnapManager erstellt für jedes Backup zwei Snapshot-Kopien. Wenn sich alle von der Datenbank benötigten Dateien in einem einzigen Volume befinden, werden beide Snapshot-Kopien in diesem Volume angezeigt.

Wenn Sie eine vollständige Sicherung angeben, führt SnapManager die folgenden Aktionen durch:

1. Platziert die gesamte Datenbank in den Online-Backup-Modus
2. Erstellt Snapshot Kopien aller Volumes, die Datenbankdateien enthalten
3. Modus für Online-Backups wird die Datenbank aus dem Online-Backup entfernt
4. Erzwingt einen Protokollschalter und archiviert dann die Protokolldateien

   Dies überträgt auch die Redo-Informationen auf die Festplatte.

5. Generiert Backup-Kontrolldateien
6. Erstellt eine Snapshot Kopie der Log-Dateien und der Backup-Kontrolldateien

Während eines vollständigen Backups wird die gesamte Datenbank von SnapManager in den Online-Backup-Modus versetzt. Ein einzelner Tablespace (z. B. E:\Data\ts1_1.dbf) befindet sich länger im Online-Backup-Modus als bestimmte Tabellen oder Datendateien, die angegeben wurden.

Wenn eine Datenbank in den Backup-Modus wechselt, schreibt Oracle ganze Blöcke in die Protokolle und schreibt nicht nur das Delta zwischen Backups. Da Datenbanken im Online Backup-Modus mehr Arbeit leisten, stellt die Auswahl eines vollständigen Backups eine größere Last für den Host dar.

Obwohl die Durchführung vollständiger Backups eine größere Belastung des Hosts bewirkt, benötigen vollständige Backups weniger Snapshot-Kopien, was zu weniger Storage-Anforderungen führt.

Teilweise Online-Backups

Anstelle eines kompletten Backups können Sie wählen, ob Sie ein partielles Backup der Tabellen in einer Datenbank durchführen möchten. Während SnapManager eine Snapshot Kopie von Volumes für *Full* Backups erstellt, erstellt SnapManager für *partial*

Backups eine Snapshot Kopie von jedem angegebenen Tablespace.

Da die Ebene des Tablespaces die unterste Ebene ist, die Oracle den Backup-Modus ermöglicht, verarbeitet SnapManager Backups auf Ebene des Tablespaces, auch wenn Sie eine Datendatei in einem Tablespace angeben.

Bei einem partiellen Backup ist jeder Tablespace im Backup-Modus für eine kürzere Zeit im Vergleich zu einem vollständigen Backup vorhanden. Während eines Online-Backups steht die Datenbank Benutzern jederzeit zur Verfügung. Die Datenbank muss jedoch mehr Arbeit erledigen, und der Host muss mehr physische I/O-Vorgänge durchführen Außerdem erstellt SnapManager Snapshot-Kopien von jedem angegebenen Tablespaces oder jedem Tablespace, der eine angegebene Datendatei anstelle des gesamten Volume enthält, mehr Snapshot Kopien.

SnapManager nimmt Snapshot Kopien bestimmter Tabellen oder Datendateien in Anspruch. Der partielle Backup-Algorithmus ist eine Schleife, die SnapManager wiederholt, bis eine Snapshot-Kopie von jedem angegebenen Tablespace oder einer Datendatei erstellt wurde.

Obwohl Sie eine partielle Sicherung durchführen können, wird empfohlen, immer eine vollständige Sicherung der gesamten Datenbank durchzuführen.

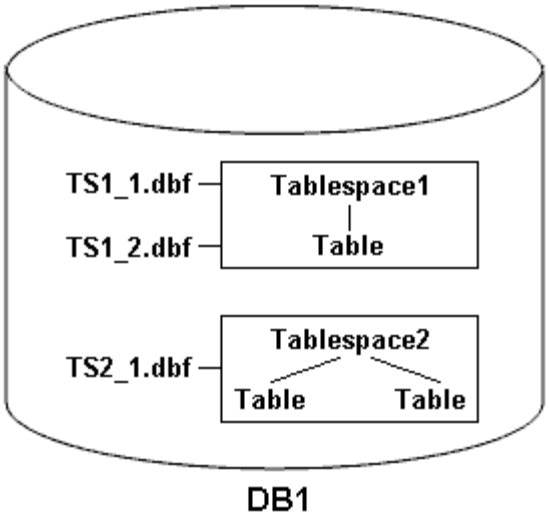
SnapManager führt während eines partiellen Backups folgende Aktionen durch:

1. Platziert den Tablespaces, der die Datendateien enthält, in den Backup-Modus.
2. Erstellt eine Snapshot-Kopie aller Volumes, die vom Tablespace verwendet werden.
3. Entfernt den Tablespace aus dem Backup-Modus.
4. Setzen Sie diesen Prozess fort, bis eine Snapshot Kopie aller Tabellen oder Dateien erstellt wurde.
5. Erzwingt einen Protokollschalter und archiviert dann die Protokolldateien.
6. Generiert Backup-Kontrolldateien
7. Erstellt eine Snapshot Kopie der Log-Dateien und der Backup-Kontrolldateien.

Beispiele für Backup-, Restore- und Recovery-Vorgänge

Hier finden Sie Informationen zu Backup-, Restore- und Recovery-Szenarien, mit denen Sie Ihre Datensicherungsziele erreichen.

In der folgenden Abbildung wird der Inhalt des Tablespaces angezeigt:



In der Abbildung hat Tablespace1 eine Tabelle und zwei Datenbankdateien mit ihr verknüpft. Tablespace2 hat zwei Tabellen und eine Datenbankdatei zugeordnet.

In der folgenden Tabelle werden einige vollständige und teilweise Backup-, Restore- und Recovery-Szenarien beschrieben:

Beispiele für vollständige Backup-, Restore- und Recovery-Vorgänge

Vollständiges Backup	Wiederherstellen	Recovery
SnapManager erstellt eine Datensicherung aller Komponenten in Datenbank DB1, einschließlich der Datendateien, Archivprotokolle und Kontrolldateien.	Vollständiges Restore mit Kontrolldateien SnapManager stellt alle Datendateien, Tablespaces und Kontrolldateien im Backup wieder her.	Sie können eine der folgenden Optionen angeben: • SCN - Geben Sie ein SCN ein, z. B. 384641. • Datum/Uhrzeit – Geben Sie ein Datum und eine Uhrzeit des Backups ein, z. B. 2005-11-25:19:06:22. • Der letzten Transaktion, die zur Datenbank durchgeführt wurde.
Vollständiges Restore ohne Kontrolldateien SnapManager stellt alle Tabellen und Datendateien ohne die Kontrolldateien wieder her.	Bei der Wiederherstellung von Datendateien oder Tablespaces mit Kontrolldateien geben Sie eine der folgenden Optionen an: • Tablespaces • Datendateien	SnapManager stellt die Daten zur letzten Transaktion wieder her, die zur Datenbank durchgeführt wurde.

Beispiele für partielle Backup-, Restore- und Recovery-Vorgänge

Teilweise Sicherung	Wiederherstellen	Recovery

Sie können eine der folgenden Optionen auswählen: • Tablespaces Sie können Tablespace1 und Tablespace2 oder nur einen von ihnen festlegen. • Datendateien Sie können alle drei Datenbankdateien (TS1_1.dbf, TS1_2.dbf und TS2_1.dbf), zwei Dateien oder eine Datei angeben. Unabhängig von der gewählten Option umfasst das Backup alle Kontrolldateien. Archivprotokolldateien sind in der Teilsicherung enthalten, wenn das Profil nicht aktiviert ist, um die Archiv-Log-Backups separat zu erstellen.	Beim Complete Restore SnapManager werden alle Datendateien, Tablespaces und Kontrolldateien, die im partiellen Backup angegeben sind, wiederhergestellt.	SnapManager stellt die Daten für die letzte Transaktion wieder her, die zur Datenbankinstanz durchgeführt wurde.

Stellen Sie entweder Datendateien oder Tablespaces mit Kontrolldateien wieder her SnapManager führt eine der folgenden Restores durch: • Alle angegebenen Datendateien • Alle angegebenen Tablespaces	Stellen Sie entweder Datendateien oder Tablespaces ohne Kontrolldateien wieder her SnapManager führt eine der folgenden Restores durch: • Tablespaces Geben Sie einen beliebigen Tablespaces an. SnapManager stellt nur die angegebenen Tablespaces wieder her. Wenn das Backup Tablespace1 enthält, stellt SnapManager nur diese Tablespaces wieder her. • Datendateien Geben Sie eine der Datenbankdateien an. SnapManager stellt nur die angegebenen Datendateien wieder her. Wenn das Backup Datenbankdateien enthält (TS1_1.dbf und TS1_2.dbf), stellt SnapManager nur diese Dateien wieder her.	Stellen Sie nur Kontrolldateien wieder her

Über die Handhabung von Steuerdateien und Archivprotokolldateien

SnapManager enthält die Kontrolldateien und enthält optional Archivprotokolldateien für jedes Backup. Archivprotokolldateien werden für Recovery-Vorgänge verwendet.

Die Datenbank verwendet Steuerdateien, um Namen, Standorte und Größe der Datenbankdateien zu identifizieren. SnapManager umfasst in jedem Backup Kontrolldateien, da beim Restore-Prozess Kontrolldateien verwendet werden.

Die Änderungen an einer Datenbank werden mithilfe der Online-Wiederherstellungsprotokolle verfolgt, die schließlich archiviert und als archivierte Wiederherstellungsprotokolle (oder Archivprotokolle) bekannt sind. SnapManager (3.2 oder höher) ermöglicht Ihnen das separate Backup von Datendateien und die Archivierung von Protokolldateien mit verschiedenen Aufbewahrungs- und Frequenzbereichen. SnapManager kann Backups nur der Archivprotokolle oder kombinierten Backups von Datendateien und Archivprotokollen erstellen. SnapManager bietet umfassendes, automatisiertes Management von Archivprotokollen und manuelle Eingriffe in das Datenbank-Recovery und ermöglicht nach dem Backup auch die Erstellung von Archivprotokollen von einem oder mehreren Archivprotokollzielen.

Um anzuzeigen, welche Tabellen und Datendateien in ein Backup enthalten sind, verwenden Sie den Befehl Backup show oder das Fenster Backup Properties.

Die folgende Tabelle zeigt, wie SnapManager Protokolldateien während jeder Ausführung und Archivierung verarbeitet:

Art des Vorgangs	Kontrolldateien	Archivierung von Protokolldateien
Backup	Bei jedem Backup enthalten	Kann bei jedem Backup berücksichtigt werden
Wiederherstellen	Sowohl allein als auch zusammen mit den Tabellen oder Datendateien können wiederhergestellt werden	Kann für den Wiederherstellungsprozess verwendet werden

Was ist für ein Datenbank-Backup geplant

Sie können Backups für Datenbanken mithilfe der Registerkarte Zeitplan der grafischen Benutzeroberfläche planen, aktualisieren und überwachen.

Die folgende Tabelle behandelt einige häufig gestellte Fragen zur Zeitplanung:

Frage	Antwort
Was geschieht mit den geplanten Backups, wenn der SnapManager Server neu gestartet wird?	Beim Neustart des SnapManager-Servers werden alle Zeitpläne automatisch neu gestartet. SnapManager wird jedoch nicht zu verpassten Vorkommnissen nachgehen.

Was geschieht, wenn zwei Backups gleichzeitig auf zwei Datenbanken geplant werden?	SnapManager startet die Backup-Vorgänge nacheinander und ermöglicht es dann, die Backups parallel auszuführen. Wenn ein Datenbankadministrator beispielsweise sechs tägliche Backup-Pläne für sechs verschiedene Datenbankprofile erstellt, die um 1:00 Uhr stattfinden, werden alle sechs Backups parallel ausgeführt. Wenn für einen kurzen Zeitraum mehrere Backups auf einem einzelnen Datenbankprofil geplant werden, führt der SnapManager-Server nur den Backup-Vorgang mit der längsten Aufbewahrungsdauer aus. Vor dem Starten eines Backup-Vorgangs legt SnapManager zunächst Folgendes fest: • Hat ein anderer Zeitplan in den letzten 30 Minuten erfolgreich ein Backup mit größerer Aufbewahrung für dasselbe Profil erstellt? • Wird ein anderer Zeitplan innerhalb der nächsten 30 Minuten versuchen, ein Backup mit größerer Aufbewahrung für dasselbe Profil zu erstellen? Wenn die Antwort auf eine der Fragen „Ja“ lautet, wird das Backup von SnapManager übersprungen. Beispielsweise kann ein Datenbankadministrator einen täglichen, wöchentlichen und monatlichen Zeitplan für ein Datenbankprofil erstellen, der alle Backups um 1:00 Uhr vorbestimmt sind An diesem Tag des Monats, an dem drei Backups gleichzeitig um 1:00 Uhr stattfinden sollen, führt SnapManager nur den Backup-Vorgang aus, der auf dem monatlichen Zeitplan basiert. Das Zeitfenster von 30 Minuten kann in einer SnapManager-Eigenschaftendatei geändert werden.
Unter welchem Benutzer wird die Sicherung ausgeführt?	Der Vorgang wird unter dem Benutzer ausgeführt, der den Zeitplan erstellt hat. Sie können dies jedoch in Ihre eigene Benutzer-ID ändern, wenn Sie sowohl für das Datenbankprofil als auch für den Host gültige Anmeldeinformationen haben. Durch das Starten von geplanten Backup-Eigenschaften für den von Avida Davis erstellten Backup-Zeitplan kann Stella Morrow beispielsweise seine Benutzer-ID für diesen Vorgang als Benutzer auswählen, um das geplante Backup auszuführen.

Wie funktioniert der SnapManager Scheduler mit dem systemeigenen Scheduler?	Auf dem SnapManager-Server können Sie die geplanten Backups nicht über den systemeigenen Scheduler des Betriebssystems anzeigen. Wenn Sie beispielsweise ein geplantes Backup erstellen, wird im Fenster geplante Aufgaben kein neuer Eintrag angezeigt.

Was passiert, wenn die Uhren in der grafischen Benutzeroberfläche und der Server nicht synchronisiert sind?	Die Uhren auf Client und Server werden nicht synchronisiert. So können Sie ein Backup planen, bei dem sich die Startzeit künftig auf dem Client, aber in der Vergangenheit auf dem Server befindet. Bei wiederkehrenden Backups erfüllt der Server die Anforderung immer noch. Wenn der Server beispielsweise eine Anfrage zur Durchführung stündlicher Backups erhält, beginnend mit einem 01/30/08 um 3:00 Uhr Aber die aktuelle Zeit ist 3:30 Uhr An diesem Tag führt der Server sein erstes Backup um 4:00 Uhr durch Und führt weiterhin Backups jede Stunde durch. Für einmalige Backups übernimmt der Server jedoch die Anfrage wie folgt: • Wenn sich die Startzeit innerhalb der letzten fünf Minuten nach der aktuellen Serverzeit befindet, beginnt SnapManager sofort mit dem Backup. • Wenn die Startzeit größer als fünf Minuten ist, startet SnapManager das Backup nicht. Betrachten wir zum Beispiel das folgende Szenario: • Die Uhr im Host der grafischen Schnittstelle liegt drei Minuten hinter der eigentlichen Zeit. • Die aktuelle Zeit auf dem Client ist 8:58 Uhr • Sie planen, ein einmalig auszusichertes Backup um 9:00 Uhr zu erstellen • Sie planen ein weiteres, einmalig zu besichertes Backup um 8:30 Uhr Wenn der Server die erste Anforderung erhält, ist die Uhrzeit auf dem Server 9:01 Uhr Obwohl sich die Startzeit für das Backup in der Vergangenheit befindet, führt SnapManager sofort das Backup durch. Wenn der Server die zweite Anforderung erhält, beträgt der Startzeit des Backups mehr als fünf Minuten in der Vergangenheit. Sie erhalten eine Meldung, dass die Terminanfrage fehlgeschlagen ist, da die Startzeit in der Vergangenheit liegt. Sie können die Zeit von fünf Minuten in einer SnapManager-Eigenschaftendatei ändern.
Was geschieht mit den geplanten Backups für ein Profil, wenn das Profil gelöscht wird?	Wenn ein Datenbankprofil gelöscht wird, löscht der SnapManager-Server geplante Backups, die für dieses Profil definiert wurden.

Wie verhalten sich geplante Backups während der Sommerzeit oder bei einer Änderung der SnapManager Serverzeit?	SnapManager Backup-Zeitpläne sind aufgrund der Sommerzeit oder beim Ändern der SnapManager Server-Zeit betroffen. Berücksichtigen Sie bei einer Änderung der Uhrzeit des SnapManager-Servers folgende Auswirkungen: • Nachdem der Backup-Zeitplan ausgelöst wurde, falls der SnapManager Server wieder zurückfällt, wird der Backup-Zeitplan nicht wieder ausgelöst. • Wenn die Sommerzeit vor der geplanten Startzeit beginnt, werden die Backup-Pläne automatisch ausgelöst. • Wenn Sie sich zum Beispiel in den USA befinden, planen Sie stündliche Backups um 4:00 Uhr Dies sollte alle 4 Stunden stattfinden. Backups werden um 4 Uhr, 8 Uhr, 12 Uhr, 4 Uhr, 8 Uhr und Mitternacht an den Tagen vor und nach der Sommerzeit im März und November durchgeführt. • Beachten Sie Folgendes, wenn die Backups für 2:30 Uhr geplant sind Jede Nacht: ◦ Wenn die Uhren eine Stunde zurückfallen, da das Backup bereits ausgelöst wurde, wird das Backup nicht erneut ausgelöst. ◦ Wenn die Uhren eine Stunde vorwärts springen, löst das Backup sofort aus. Wenn Sie sich in den USA befinden und dieses Problem vermeiden möchten, müssen Sie Ihre Backups so planen, dass sie außerhalb von 2:00 Uhr beginnen Bis 3:00 Uhr Intervall:

Datenbank-Backups werden erstellt

Backups von ganzen Datenbanken oder Teilen von Datenbanken, einschließlich Tabellen, Datendateien oder Kontrolldateien, können erstellt werden.

Administratoren können optional Backups mit Oracle RMAN registrieren, um die Datenbank mit granulareren Besonderheiten wie Blöcken wiederherzustellen.

Sie können die Namen der Snapshot Kopien, die durch Backups dieses Profils erstellt werden, während Sie dieses Profil definieren. Beispielsweise können Sie eine Präfixzeichenfolge mit HOPS einfügen, um High Operations Backups zu kennzeichnen.

Sie können nicht nur eindeutige Namen für Snapshot Kopien definieren, die durch Backups erstellt werden, sondern auch eindeutige Bezeichnungen für die Backups selbst erstellen. Wenn Sie ein Backup erstellen, ist es eine gute Praxis, einen Namen für das Backup anzugeben, so dass Sie eine einfache Möglichkeit haben, es mit dem Parameter -Label zu identifizieren. Dieser Name muss für alle Backups, die innerhalb eines bestimmten Profils erstellt wurden, eindeutig sein. Der Name kann Buchstaben, Zahlen, Unterstrich (_) und Bindestrich (-) enthalten. Es kann nicht mit einem Bindestrich beginnen. Bei Etiketten wird die Groß-/Kleinschreibung beachtet. Möglicherweise möchten Sie Informationen wie Umgebungsvariablen des

Betriebssystems, Systemdatum und Backup-Typ anhängen.

Wenn Sie kein Etikett bereitstellen, erstellt SnapManager im Formular scope_Mode_datestring einen Standardnamen mit dem Namen scope_Mode_datestring, wobei der Umfang voll oder teilweise ist und der Modus offline, online oder automatisch ist (der Buchstabe c für kalt, h für heiß oder A für automatisch).

Ab SnapManager 3.4 können Sie Ihr eigenes Backup-Label bereitstellen, indem Sie das von SnapManager erstellte Standard-Backup-Label überschreiben. Sie müssen den Wert des Parameters override.default.backup.pattern auf true setzen und im Parameter new.default.backup.pattern die neue Sicherungsbezeichnung angeben. Das Backup-Label-Muster kann Schlüsselwörter wie Datenbankname, Profilname, Umfang, Modus und Hostname enthalten, die durch Unterstrich getrennt werden müssen. Beispiel: new.default.backup.pattern=dbname_profile_hostname_scope_mode.

Der Zeitstempel wird automatisch am Ende des generierten Etiketts eingefügt.

Wenn Sie einen Kommentar eingeben, können Sie Leerzeichen und Sonderzeichen enthalten. Wenn Sie hingegen ein Etikett eingeben, enthalten Sie keine Leerzeichen oder Sonderzeichen.

Für jedes Backup generiert SnapManager automatisch eine GUID, eine 32-stellige HEX-Zeichenfolge. Zum Bestimmen der GUID müssen Sie den Befehl für die Sicherungsliste mit der Option -wortrecih ausführen.

Sie können eine vollständige Sicherung einer Datenbank erstellen, während diese online oder offline ist. Um SnapManager mit der Sicherung einer Datenbank umgehen zu lassen, unabhängig davon, ob sie online oder offline ist, sollten Sie die Option -Auto verwenden.

Wenn Sie beim Erstellen eines Backups die Beschneidung aktiviert haben und die zusammenfassende Benachrichtigung im Profil aktiviert wurde, werden zwei separate E-Mails ausgelöst. Eine E-Mail ist für den Backup-Vorgang und die andere für die Beschneidung. Sie können diese E-Mails korrelieren, indem Sie den Backup-Namen und die Backup-ID in diesen E-Mails vergleichen.

Sie können ein Cold Backup erstellen, wenn sich die Datenbank im Shutdown-Status befindet. Wenn sich die Datenbank in einem gemounteten Zustand befindet, ändern Sie sie in einen Shutdown-Status, und führen Sie das Offline-Backup (Cold Backup) durch.

Mit SnapManager (3.2 oder höher) können Sie die Archivprotokolldateien getrennt von den Datendateien sichern und so die Archivprotokolldateien effizient verwalten.

Um die Backups des Archivprotokolls separat zu erstellen, müssen Sie ein neues Profil erstellen oder das bestehende Profil aktualisieren, um die Backup des Archivprotokolls mit der Option -separatem-archivlog -Backups zu trennen. Mithilfe des Profils können Sie die folgenden SnapManager-Vorgänge durchführen:

- Erstellen Sie eine Backup-Datei für Archivprotokolle.
- Löschen Sie eine Sicherung des Archivprotokolls.
- Mounten Sie ein Backup für das Archivprotokoll.
- Kostenlose Backup eines Archivprotokolls.

Die Backup-Optionen variieren je nach Profileinstellungen:

- Mit einem Profil, das nicht getrennt ist, um Archiv-Log-Backups separat durchzuführen, können Sie Folgendes tun:
  - Erstellen Sie ein vollständiges Backup.
  - Erstellen Sie ein partielles Backup.

- Geben Sie für Archivprotokolldateien zu sichernde Ziele an.
- Geben Sie Archivprotokollziele an, die vom Backup ausgeschlossen werden sollen.
- Legen Sie die Beschneiungsoptionen für das Löschen der Archivprotokolldateien aus den Archivprotokollzielen fest.

- Mithilfe eines Profils, das zur Erstellung von Archiv-Log-Backups getrennt ist, können Sie Folgendes tun:
  - Erstellen Sie ein Backup nur für Datendateien.
  - Erstellen Sie ein Backup nur archivels.
  - Während Sie ein Backup nur für Datendateien erstellen, schließen Sie das Backup des Archivprotokolls zusammen mit den online gespeicherten Datendateien nur zum Klonen ein.

    Wenn Sie Archiv-Log-Backups zusammen mit Datendateien auf der Seite **Profileinstellungen** des Assistenten **Profile Create** der SnapManager-Benutzeroberfläche enthalten haben, Und wenn Sie die Option **Archivierungsprognogs** im Assistenten * Backup Create* nicht ausgewählt haben, erstellt SnapManager immer das Archiv-Log Backup zusammen mit Datendateien für alle Online-Backups.

    In einer solchen Situation können Sie über die SnapManager-CLI alle Ziele für das Archiv-Protokoll für die Sicherung außer den in der SnapManager-Konfigurationsdatei angegebenen Ausschlusszielen betrachten. Aber Sie können diese Archiv-Log-Dateien nicht beschneiden. Allerdings können Sie immer noch die Option -archivoogs verwenden, um das Ziel der Archivprotokolldatei anzugeben und die Archivprotokolldateien von der SnapManager CLI zu beschneiden.

    Wenn Sie die Datensicherung mit der Option -Auto erstellen und die Option --archivprotokolle angeben, erstellt SnapManager entweder ein Online- oder Offline-Backup auf Grundlage des aktuellen Status des Backups.

    - SnapManager erstellt ein Offline Backup, wenn die Datenbank offline ist und keine Archivprotokolldateien in das Backup berücksichtigt.
    - SnapManager erstellt ein Online Backup einschließlich Archiv-Log-Dateien, wenn die Datenbank online ist.
  - Während das nur Archivprotokolle erstellt wird:
    - Geben Sie das Archivprotokoll-Ziel an, das gesichert werden soll, zusammen mit dem nur-Archivprotokoll-Backup
    - Geben Sie die Ziele für das Archivprotokoll an, die vom Backup nur für Archivprotokolle ausgeschlossen werden sollen
    - Legen Sie die Beschneiungsoptionen für das Löschen der Archivprotokolldateien aus den Archivprotokollzielen fest
- **Szenarien nicht unterstützt**
  - Sie können das nur-Archivprotokoll-Backup nicht zusammen mit einem Offline-Datendatei-Backup erstellen.
  - Sie können die Archivprotokolldateien nicht beschneiden, wenn die Archivprotokolldateien nicht gesichert sind.
  - Sie können die Archivprotokolldateien nicht beschneiden, wenn der Flash Recovery Area (FRA) für Archivprotokolldateien aktiviert ist.

    Wenn Sie im Bereich Flash Recovery den Speicherort für das Archivprotokoll angeben, müssen Sie im Parameter Archive_log_dest auch den Speicherort für das Archivprotokoll angeben.

Während Sie Backups für Archivprotokolle erstellen, müssen Sie die vollständigen Pfade für Archivprotokolle in doppelten Anführungszeichen und den Zielpfaden eingeben, die durch Kommas getrennt sind. Der Pfadtrenner sollte als zwei umgekehrte Schrägstriche (\\) anstelle eines angegeben werden.

Wenn Sie das Label für die Sicherung von Online-Datendateien mit dem enthaltenen Archiv-Log-Backup angeben, wird das Etikett für die Datensicherung von Datendateien angewendet, und das Archiv-Log-Backup wird mit (_logs) aufgestickt. Dieses Suffix kann konfiguriert werden, indem der Parameter Suffix.Backup.Label.with.logs in der SnapManager-Konfigurationsdatei geändert wird.

Sie können beispielsweise den Wert als Suffix.Backup.Label.with.logs=Arc angeben, sodass der Standardwert _logs in _Arc geändert wird.

Wenn Sie keine Ziele für das Archivprotokoll angegeben haben, die in das Backup aufgenommen werden sollen, enthält SnapManager alle in der Datenbank konfigurierten Archivprotokollziele.

Wenn in einem der Ziele keine Archivprotokolldateien fehlen, überspringt SnapManager alle diese Archivprotokolldateien, die vor den fehlenden Archivprotokolldateien erstellt wurden, selbst wenn diese Dateien in anderen Archivprotokollzielen verfügbar sind.

Während der Erstellung von Archiv-Log-Backups müssen Sie die Ziele für die Archivprotokolldatei angeben, die in die Sicherung aufgenommen werden sollen, und können den Konfigurationsparameter so einstellen, dass die Archivprotokolldateien immer über die fehlenden Dateien in der Sicherung hinausgehen.

Standardmäßig ist dieser Konfigurationsparameter auf true gesetzt, um alle Archivprotokolldateien über fehlende Dateien hinaus einzubeziehen. Wenn Sie Ihre eigenen Archiv-Log-Beschneidungsskripte verwenden oder Archivprotokolldateien manuell aus den Archiv-Protokollzielen löschen, können Sie diesen Parameter deaktivieren, damit SnapManager die Archivprotokolldateien überspringen und weiter mit der Sicherung fortfahren kann.

SnapManager unterstützt die folgenden SnapManager Vorgänge für Backups des Archivprotokolls nicht:

- Klonen der Backup des Archivprotokolls
- Backup des Archivprotokolls wiederherstellen
- Backup des Archivprotokolls überprüfen

SnapManager unterstützt auch die Sicherung der Archivprotokolldateien aus den Zielen des Flash-Recovery-Bereichs.

1. Geben Sie den folgenden Befehl ein: bbs Backup create -profile_Name {[-full {-online} -offline} [-contake {-hourly — Weekly { -unlimited}] [-verify] [-dataces [[-filesfiles [files] [-Tabellen-Tabellen [-Tabellen]] [-datalabellabel] {-online [-offline-} [-contake-monthly-commocellabel] [-Backup-destpath1 [,[path2]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all {}}} -untilSCN - bis-Datum yyyyy-MM-dd:HH:mm:ss [-deplune-destprune] [-depose-depose] [-despune-depose]

Ihr Ziel ist	Dann…

Geben Sie an, ob Sie eine Sicherung einer Online- oder Offline-Datenbank durchführen möchten, anstatt SnapManager zu erlauben, ob es online oder offline ist	Geben Sie -offline an, um eine Sicherung der Offline-Datenbank zu erstellen. Geben Sie -online an, um eine Sicherung der Online-Datenbank durchzuführen. + Wenn Sie diese Optionen verwenden, können Sie die Option -Auto nicht verwenden.
Geben Sie an, ob SnapManager die Sicherung einer Datenbank handhaben soll, unabhängig davon, ob sie online oder offline ist	Geben Sie die Option -Auto an. Wenn Sie diese Option verwenden, können Sie die Option --offline oder -online nicht verwenden.

Geben Sie an, ob Sie eine partielle Sicherung bestimmter Dateien durchführen möchten	`Specify the -data-files option and then list the files, separated by commas. For example, list the file names f1, f2, and f3 after the option.`
	`+ Beispiel für die Erstellung einer partiellen Datendatei-Sicherung unter Windows`
	
	+
	
	`smo backup create -profile nosep -data -files "J:\\mnt\\user\\user.dbf" -online -label partial_datafile_backup -verbose`

Geben Sie an, ob Sie eine partielle Sicherung bestimmter Tabellen durchführen möchten	``` Specify the -data-tablespaces option and then list the tablespaces, separated by commas. For example, use ts1, ts2, and ts3 after the option. + SnapManager unterstützt das Backup von schreibgeschützten Tablespaces. Beim Erstellen des Backups ändert SnapManager die schreibgeschützten Tabellenbereiche zu lesen/schreiben. Nach dem Erstellen des Backups werden die Tabellen auf schreibgeschützt geändert. ``` + Beispiel zum Erstellen einer Datensicherung für Teiltablespaces + ``` smo backup create -profile nosep -data -tablespaces tb2 -online -label partial_tablespace_bkup -verbose ```
Geben Sie an, ob Sie für jedes Backup ein eindeutiges Label im folgenden Format erstellen möchten: Full_Hot_mybackup_Label	``` For Windows, you might enter this example: ``` + ``` smo backup create -online -full -profile targetdb1_prof1 -label full_hot_my_backup_label -verbose ```

Geben Sie an, ob Sie eine Sicherungskopie der Archivprotokolldateien getrennt von den Datendateien erstellen möchten	``` Specify the following options and variables: ** -Archivalogs erstellt eine Sicherung der Archiv-Log-Dateien. ** -Backup-dest gibt die Ziele für die Archivprotokolldatei an, die gesichert werden sollen. ** -Exclude-dest gibt die zu ausgeschlossenen Archivprotokollziele an. ** -Label gibt die Bezeichnung für die Sicherung der Archivprotokolldatei an. *Hinweis:* Sie müssen entweder die Option -Backup-dest oder die Option -exclude-dest angeben. ``` + Wenn Sie beide Optionen zusammen mit der Fehlermeldung „Backup zeigt“ angeben, haben Sie eine ungültige Backup-Option angegeben. Geben Sie eine der Optionen an: -Backup-dest oder exclude-dest. + Beispiel für das Erstellen von Backups von Archivprotokolldateien getrennt unter Windows + ``` smo backup create -profile nosep -archivelogs -backup-dest "J:\\mnt\\archive_dest_2\\" -label archivelog_backup -verbose ```

Geben Sie an, ob Sie eine Datensicherung der Datendateien erstellen und Protokolldateien archivieren möchten	``` Specify the following options and variables: ** -Data Option, um die Datendateien anzugeben. ** -Archivalogs Option zur Angabe der Archiv-Log-Dateien. Beispiel für die gemeinsame Sicherung von Datendateien und Archivprotokolldateien unter Windows ``` + ``` smo backup create -profile nosep -data -online -archivelogs -backup-dest "J:\\mnt\\archive_dest_2\\" -label data_arch_backup -verbose ```

| **Geben Sie an, ob Sie die Archiv-Log-Dateien beim Erstellen eines Backups beschneiden möchten** | ```
 Specify the following options and variables:
** -Prunelogs gibt an, die Archiv-Log-Dateien aus den Archiv-Log-Zielen zu löschen.
```<br><br>+ **\* -All gibt an, alle Archiv-Log-Dateien aus den Archiv-Log-Zielen zu löschen.** \* -Bis-scntabis-scn gibt an, die Archivprotokolldateien bis zu einem angegebenen SCN zu löschen. **\* -Until-dateyyyyy-MM-dd:HH:mm:ss gibt an, die Archiv-Log-Dateien bis zum angegebenen Zeitraum zu löschen.** \* -Before gibt an, die Archivprotokolldateien vor dem angegebenen Zeitraum zu löschen (Tage, Monate, Wochen, Stunden). **\*** -Prune-destprune_dest1,[prune_dest2 gibt an, die Archiv-Log-Dateien aus den Archiv-Protokollzielen zu löschen, während die Sicherung erstellt wird. **Hinweis:** die Archivprotokolldateien können nicht beschnitten werden, wenn der Flash Recovery Area (FRA) für Archiv-Log-Dateien aktiviert ist.<br><br>+ Beispiel für das Beschneiden aller Archiv-Log-Dateien während der Erstellung einer Sicherung unter Windows<br><br>+<br><br>+<br><br>+<br><br>```
smo backup create -profile nosep
 -archivelogs -label
archive_prunebackup1 -backup-dest
"E:\\oracle\\MDV\\oraarch\\MDVarc
h,J:\\
" -prunelogs -all -prune-dest
"E:\\oracle\\MDV\\oraarch\\MDVarc
h,J:\\" -verbose
``` |
| **Geben Sie an, ob Sie einen Kommentar zum Backup hinzufügen möchten** | „Specify -comment“ gefolgt von der Beschreibungstext. |

Geben Sie an, ob Sie die Datenbank in den Zustand zwingen möchten, den Sie angegeben haben, um sie zu sichern, unabhängig davon, in welchem Zustand sie sich derzeit in befindet	Geben Sie die Option -Force an.
Geben Sie an, ob Sie das Backup gleichzeitig überprüfen möchten, wenn Sie es erstellen	Geben Sie die Option -verify an.
Geben Sie an, ob Sie die Dump-Dateien nach dem Datenbank-Backup-Vorgang sammeln möchten	Geben Sie die -dump-Option am Ende des Befehls zum Erstellen von Backups an.

Beispiel

```
smo backup create -profile targetdb1_prof1 -full -online -force  -verify
```

Verwandte Informationen

Benennen von Snapshot-Kopien

Erstellen von vor-, Post-Task- und Richtlinienskripten

Aufgabenskripte werden erstellt

Speichern der Taskskripte

Der Befehl smo Backup erstellen

Erstellen oder Aktualisieren der Postskripte

Beschneiden von Archivprotokolldateien

Sie können die Archiv-Log-Dateien aus den Archiv-Log-Speicherorten beschneiden, während Sie eine Sicherung erstellen.

- Archivprotokolldateien müssen durch den aktuellen Backup-Vorgang gesichert werden.

  Wenn der Beschnitt zusammen mit anderen Backups angegeben wird, die keine Archivprotokolldateien enthalten, werden die Archivprotokolldateien nicht beschnitten.

- Die Datenbank muss sich im angehängten Status befinden.

  Wenn die Datenbank nicht angehängt ist, geben Sie die Option -Force zusammen mit dem Backup-Befehl ein.

Während eines Backup-Vorgangs können Sie Folgendes angeben:

- Beschnitt:
  - Löschen Sie alle Archivprotokolldateien.

- Löschen Sie die Archivprotokolldateien bis zur angegebenen Systemänderungsnummer (SCN).
- Löschen Sie die Archivprotokolldateien bis zum angegebenen Zeitpunkt.
- Löschen Sie die Archivprotokolldateien vor dem angegebenen Zeitraum.

- Ziel, von dem die Archivprotokolldateien beschnitten werden müssen.

> Selbst wenn die Archivprotokolldatei Beschnitt in einem Ziel fehlschlägt, beschnitten SnapManager weiterhin die Archivprotokolldateien von den anderen Zielen.

Vor dem Löschen der Archivprotokolldateien überprüft SnapManager Folgendes:

- Archivprotokolldateien werden mindestens einmal gesichert.
- Archivprotokolldateien werden, falls vorhanden, an die Oracle Dataguard Standby-Datenbank gesendet.
- Archivprotokolldateien werden, falls vorhanden, durch den Oracle Stream-Erfassungsprozess erfasst.

Wenn die Archivprotokolldateien gesichert, in den Standby-Modus versetzt und vom Erfassungsprozess erfasst werden, löscht SnapManager alle Archivprotokolldateien in einer einzigen Ausführung. Wenn es jedoch Archivprotokolldateien gibt, die nicht gesichert, nicht in den Standby-Modus geliefert oder nicht durch den Erfassungsprozess erfasst werden, löscht SnapManager die Archivprotokolldateien nacheinander. Das Löschen von Archivprotokollen-Dateien in einer einzigen Ausführung ist schneller als das Löschen von Archivprotokollen.

SnapManager kann auch die Archivprotokolldateien gruppieren und Batch-by-Batch löschen. Jeder Batch hat maximal 998 Dateien. Dieser Wert kann unter 998 mit dem Konfigurationsparameter Maximum.archivelog.files.toprune.atATIME in der Datei smo.config konfiguriert werden.

SnapManager verwendet zum Löschen der Archivprotokolldateien den Befehl Oracle Recovery Manager (RMAN). SnapManager ist jedoch nicht mit den RMAN Aufbewahrungsrichtlinien und Löschrichtlinien integriert.

> Wenn Sie die Archivprotokolldateien aus den Archivprotokollzielen löschen, schlägt das Beschneiden von Archivprotokolldateien fehl.

SnapManager unterstützt das Beschneiden von Archiv-Log-Dateien in den folgenden Szenarien nicht:

- Im Bereich Flash Recovery befinden sich Archivprotokolldateien.
- Archivprotokolldateien befinden sich in der Standby-Datenbank.
- Die Archivprotokolldateien werden sowohl von SnapManager als auch von RMAN gemanagt.

a. Geben Sie den folgenden Befehl ein: bbs Backup create -profile_Name {[-full {-online { -offline} [-contake {-hourly [-Daily { -Weekly} -unlimited}] [-confirm] [-dataces [-monthly-pathogabel] [-monthly-pathogabel [-monthly-pathogabel] [-laboraces-online [-online [-}] [--monthly-monthly-contaces] [] [-monthly-conceptaces-monthly-] [] [-monthly-contake] [-] [-monthly-monthly-con [,[path2]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all, -untilSCN - bis-dateyyyyy-MM-dd:HH:mm:ss} -vor {-Monaten in -Wochen}} -prune-destprune_dest1,[prune_taskest2] [-specity]

Ihr Ziel ist	Dann…

Prune Archivprotokolldateien	Legen Sie die folgenden Optionen fest: • -Prunelogs gibt an, die Archivprotokolldateien beim Erstellen einer Sicherung zu löschen. ◦ -All gibt an, alle Archiv-Log-Dateien zu löschen. ◦ -UntilSCN gibt an, die Archivprotokolldateien bis zum angegebenen SCN zu löschen. ◦ -Bis-date gibt an, dass die Archivprotokolle gelöscht werden, einschließlich des angegebenen Datums und der angegebenen Uhrzeit. ◦ -Vor {-Monaten
-Tage	-Wochen
-Hours} gibt an, dass die Archiv-Log-Dateien vor dem angegebenen Zeitraum gelöscht werden.	**Das Ziel, aus dem die Archiv-Log-Dateien beschnitten werden sollen**, sollte einbezogen werden

Konsolidierung von Backups für Archivprotokolle

SnapManager konsolidiert die nur-Archivierten Backups jedes Mal, wenn Sie ein Backup erstellen, indem die doppelten, nur-Archivierten Backups freigesetzt werden. Standardmäßig ist Konsolidierung aktiviert.

SnapManager erkennt die nur archivlog Backups, die in anderen Backups Archivprotokolle haben und gibt ihnen die Möglichkeit, eine Mindestanzahl an nur Archivprotokoll-Dateien aufrechtzuerhalten.

Wenn die nur Archivprotokolle durch Konsolidierung freigegeben werden, dann werden diese Backups basierend auf der Aufbewahrungsdauer des Archivprotokolls gelöscht.

Wenn sich die Datenbank während der Konsolidierung des Archivprotokolls im Shutdown- oder Nomount-Status befindet, ändert SnapManager die Datenbank in den Bereitstellungsstatus.

Wenn die Sicherung oder Beschneidung von Archiv-Log-Dateien fehlschlägt, dann wird die Konsolidierung nicht durchgeführt. Die Konsolidierung von nur-archivlog Backups wird nur nach erfolgreichen Backups und erfolgreichen Anstiftungen verfolgt.

1. Um die Konsolidierung der nur archivlog Backups zu ermöglichen, ändern Sie die Konfigurationsparameter-Konsolidierung und setzen Sie den Wert in der SnapManager Konfigurationsdatei (smo.config) als wahr ein.

   Sobald der Parameter festgelegt ist, werden die archivlog-only Backups konsolidiert.

   Wenn das neu erstellte Archivprotokoll-only Backup die gleichen Archivprotokolldateien in einem der früheren nur-Archivprotokolle enthält, dann werden die Backups des früheren Archivprotokolls freigegeben.

SnapManager konsolidiert nicht das Backup des Archivprotokolls, das zusammen mit dem Datendateien-Backup aufgenommen wurde. SnapManager konsolidiert das nur archivBackup.

SnapManager konsolidiert die Archiv-Log-Backups selbst dann, wenn der Benutzer die Archiv-Log-Dateien manuell aus den Archiv-Log-Zielen löscht oder wenn die Archiv-Log-Dateien beschädigt sind und möglicherweise die Sicherung enthalten.

2. Um die Konsolidierung der Archiv-Log-Backups zu deaktivieren, ändern Sie die Konfigurationsparameter-Konsolidierung und setzen Sie den Wert in der SnapManager-Konfigurationsdatei (smo.config) als false.

Planung der Beschneidung der Archivprotokolldatei

Wenn Sie ein Backup erstellen, können Sie die Beschneidung von Archivprotokolldateien für eine bestimmte Zeit planen.

Mit SnapManager können Sie die Archivprotokolldateien regelmäßig aus dem aktiven Dateisystem beschneiden.

1. Geben Sie den folgenden Befehl ein: bbs Schedule create -profile_Name {[-full {-online { -offline}[-contave [-hourly — Weekly — unlimited] [-confirm] [-data-filesfiles [files] [-pathtaces-pathtaces-tabtaces [-pathonaces] [-online [-offline}}[-patheptaces [-monthly-contaceptaces] [-monthly-pathog2] [-pathonly-pathonaces] [-pathonaces] [-pathonaces [-pathonaces] [-pathonaces] [-pathonaces] [-pathon [-prunelogs{-all -untilSCNuntilSCN} -before {-dateyyyy-MM-dd HH:mm:ss {-monthsmonths -weeksweeweeweeweeweeweeweywy-days -hoursshourshours}} -prune-destune_dest1,,prune_dest2] -datyyyyyyyyyyyyyyyyyyy_Name [-term-terate-schedule-term_term_term_runytime_runytime_runyytime_runyyyyyytime_terours { <} -mony-time -monthyyyyyyyyyyyyyyyyyyytime

Ihr Ziel ist	Dann…
Planen eines Beschneidung von Archivprotokolldateien	Legen Sie die folgenden Optionen fest: • -Prunelogs zu planen Beschneidung der Archiv-Log-Dateien • -Prune-dest Archivprotokolldateien aus den Archivprotokollzielen zu prune
• Einen Namen für den Terminplan angeben*	Geben Sie die Option -terminplan-Name an.

Planen Sie das Beschneiden von Archivprotokolldateien in einem bestimmten Zeitintervall	Geben Sie die Intervalloption an und geben Sie an, ob die Archivprotokolldateien auf der Grundlage der folgenden Intervallklassen beschnitten werden sollen: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • Nur -ontimeonly
Fügen Sie einen Kommentar über die Terminplanoperation	Geben Sie die Option -terminieren-comment an, gefolgt von der Beschreibungszeichenfolge.
Geben Sie die Startzeit der Zeitplanoperation an	Geben Sie die Option -Start-time im Format yyyy-mm-dd hh:mm an.

Was ist AutoSupport

Die AutoSupport-Funktion ermöglicht es dem SnapManager Server, nach Abschluss des Backup-Vorgangs AutoSupport Meldungen an das Storage-System zu senden.

SnapManager sendet AutoSupport-Meldungen nur für erfolgreiche Backup-Vorgänge.

Sie können AutoSupport aktivieren oder deaktivieren, indem Sie dem Konfigurationsparameter Auto_Support.on in der Konfigurationsdatei smo.config die folgenden Werte zuweisen:

- TRUE – aktiviert AutoSupport
- FALSE - deaktiviert AutoSupport

Standardmäßig ist AutoSupport in SnapManager aktiviert.

Verwandte Informationen

Hinzufügen von Storage-Systemen, die in Clustered Data ONTAP betrieben werden, zum SnapManager Server-Host

Aktivierung von AutoSupport in SnapManager

Deaktivieren von AutoSupport in SnapManager

Hinzufügen von Storage-Systemen, die in Clustered Data ONTAP betrieben werden, zum SnapManager Server-Host

Sie müssen die Storage-Systeme, die in Clustered Data ONTAP ausgeführt werden, zum SnapManager Server Host hinzufügen, um AutoSupport zu aktivieren. Ab SnapManager 3.3 wurde AutoSupport nur auf Storage-Systemen mit 7-Mode unterstützt.

1. Fügen Sie dem SnapManager-Server-Host eine Admin Storage Virtual Machine (SVM, früher als Vserver bezeichnet) und eine SVM, die in Clustered Data ONTAP betrieben wird: Sdcli Transport_Protocol set -f AdminVserver_Name oder Vserver_Name -type HTTP -user admin hinzu

   Geben Sie den folgenden Befehl ein: Die Meldung wird angezeigt.

2. Geben Sie das Passwort ein, das Sie beim Erstellen der SVM angegeben haben.

   Nachdem Sie den Befehl erfolgreich ausgeführt haben, wurde das neue Transportprotokoll festgelegt. Meldung wird angezeigt.

Aktivierung von AutoSupport in SnapManager

Sie müssen AutoSupport aktivieren, damit Storage-Systeme bei jedem erfolgreichen Backup-Vorgang Meldungen vom SnapManager-Server empfangen.

AutoSupport kann auf zwei Arten aktiviert werden:

- Standardmäßig enthält die neue Installation von SnapManager nicht den Parameter Auto_Support.on in der Konfigurationsdatei smo.config. Dies impliziert, dass AutoSupport aktiviert ist.
- Sie können den Parameter Auto_Support.on manuell konfigurieren.
  a. Beenden Sie den SnapManager-Server.
  b. Legen Sie in der Konfigurationsdatei smo.config den Wert des Parameters Auto_Support.on auf TRUE fest.

     auto_Support.on=TRUE

  c. Starten Sie den SnapManager-Server neu.

Deaktivieren von AutoSupport in SnapManager

Sie müssen AutoSupport deaktivieren, wenn das Storage-System bei jedem erfolgreichen Backup-Vorgang keine Meldungen vom SnapManager-Server empfangen soll.

Standardmäßig ist AutoSupport aktiviert, wenn die Konfigurationsdatei den Parameter Auto_Support.on nicht enthält. In diesem Szenario müssen Sie den Parameter Auto_Support.on in der Konfigurationsdatei hinzufügen und den Wert AUF FALSE setzen.

1. Beenden Sie den SnapManager-Server.
2. Legen Sie in der Konfigurationsdatei smo.config den Wert für den Parameter Auto_Support.on auf FALSE fest.

   auto_Support.on=FALSE

3. Starten Sie den SnapManager-Server neu.

Datenbank-Backups werden überprüft

Sie können mit dem Befehl Backup Verify überprüfen, ob die Blöcke im Datenbank-Backup nicht beschädigt sind. Der Verify-Vorgang ruft das Dienstprogramm Oracle

Database Verify für jede Datendatei im Backup auf.

Mit SnapManager können Sie den Verifizierungsvorgang jederzeit für Sie und die Benutzer in Ihrem System durchführen. Sie können die Verifizierung sofort nach dem Erstellen des Backups durchführen. Sie müssen das Profil angeben, das das Backup enthält, und entweder die Bezeichnung oder die ID des erstellten Backups.

Die Backup-Überprüfung schlägt in einer Windows-Umgebung fehl, wenn Sie SnapManager 3.0 und Oracle Database 11.1.0.7 verwenden. Sie müssen Oracle Database 11.2.0.1 oder höher verwenden.

Sie können -dump angeben, um die Dump-Dateien nach der Backup-Überprüfung zu sammeln.

1. Geben Sie den folgenden Befehl ein: smo Backup verify -profile profile_Name [-Label Label [-idid] [-Force] [-dump] [-quiet

Verwandte Informationen

Der Befehl smo Backup verify

Ändern der Richtlinie zur Aufbewahrung von Backups

Sie können die Eigenschaften eines Backups ändern, sodass dieser gemäß der Aufbewahrungsrichtlinie zum Löschen berechtigt oder nicht zur Verfügung steht.

Wenn Sie ein Backup erstellen, können Sie dessen Aufbewahrungsrichtlinie festlegen. Sie können später wählen, ob Sie das Backup für einen längeren Zeitraum aufbewahren möchten, als die Aufbewahrungsrichtlinie es zulässt oder angeben, dass Sie das Backup nicht mehr benötigen und die Aufbewahrungsrichtlinie es verwalten soll.

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Dauerhaft Aufbewahrung von Backups

Sie können angeben, dass ein Backup durch die Aufbewahrungsrichtlinie nicht zur Löschung berechtigt sein sollte, um das Backup auf unbestimmte Zeit zu halten.

1. Um anzugeben, dass ein Backup unbegrenzt aufbewahrt werden soll, geben Sie folgenden Befehl ein:smo Backup Update -profilprofile_Name {-labellabel [Data / -archivelogs] / -idid} -restate -unlimited

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Zuweisen von Backups mit einer bestimmten Aufbewahrungsklasse

Datenbankadministratoren können Backups mit einer bestimmten Aufbewahrungsklasse stündlich, täglich, wöchentlich oder monatlich durchführen. Durch das Zuweisen einer bestimmten Aufbewahrungsklasse können die unter dieser Änderung durchgeführten Backups gelöscht werden.

1. Um eine bestimmte Backup-Aufbewahrungs-Klasse zuzuweisen, geben Sie diesen Befehl ein:smo Backup Update -profilprofile_Name {-labellabel [Data} -archivelogs]

Ändern des Standardverhaltens der Aufbewahrungsrichtlinie

Wenn ein Backup basierend auf der Aufbewahrungsrichtlinie abläuft, bestimmt SnapManager basierend auf den Aufbewahrungseinstellungen, ob das Backup gelöscht werden soll. Das Löschen von Backups ist das Standardverhalten. Sie können dieses Standardverhalten ändern und stattdessen die ungeschützten Backups freigeben.

Standardmäßig löscht Snap Manager das Backup nach Ablauf des Backup.

1. Zugriff auf den folgenden Standardspeicherort:

   Standard smo Installation location\Properties\smo.config

2. Bearbeiten Sie die Datei smo.config.
3. Legen Sie in der Datei smo.config die Eigenschaft contee.alwayFreeExpiredBackups auf true fest.

   Beispiel: „Exkepe.alwayFreeExpiredBackups“ = „true“

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Freistellen oder Löschen von Backups ohne Rücknahmerichtlinien

Backups mit einer „unbegrenzten“ Aufbewahrungsklasse können nicht direkt gelöscht oder freigegeben werden. Um diese Backups zu löschen oder zu löschen, müssen Sie zunächst eine andere Aufbewahrungsklasse wie stündlich, täglich, wöchentlich oder monatlich zuweisen. Um ein Backup zu löschen oder zu befreien, das von der Aufbewahrungsrichtlinie ausgenommen ist, müssen Sie zuerst das Backup aktualisieren, um es für die Löschung berechtigt zu machen oder es freizumachen.

1. Um das Backup zu aktualisieren, damit es durch die Aufbewahrungsrichtlinie zum Löschen berechtigt ist, geben Sie folgenden Befehl ein: smo Backup Update -profilprofile_Name {-labellabel [Data - archivelogs] -idid} -cond [-hourly - -Weekly]
2. Nachdem Sie die Sicherung aktualisiert haben, damit sie gelöscht werden kann, können Sie entweder das Backup löschen oder kostenlose Backup-Ressourcen.
   - Um das Backup zu löschen, geben Sie folgenden Befehl ein: smo Backup delete -profilprofile_Name {-labellabel [Data} -archivelogs] - idid - all
   - Um die Backup-Ressourcen freizumachen, anstatt das Backup zu löschen, geben Sie diesen Befehl ein:smo Backup free -profileprofile_Name {-labellabel [Data} -archivelogs] [-did [-all [-Force] [-dump] [-quiet

Verwandte Informationen

Der SMO-Befehl zum Aktualisieren der Datensicherung

Anzeigen einer Liste von Backups

Sie können überprüfen, welche Backups für ein Profil und den Backup-Status erstellt wurden, indem Sie den Befehl smo Backup list verwenden. Der Befehl zeigt für jedes Profil zuerst die Informationen zum letzten Backup an und fährt dann fort, bis die Informationen für alle Backups angezeigt werden.

1. Geben Sie den folgenden Befehl ein: smo Backup list -profilprofile_Name [-dimitercharacter] [Data / -archivalogs] [-quiet

Verwandte Informationen

Der Befehl smo Backup list

Anzeigen von Backup-Details

Sie können die detaillierten Informationen über ein bestimmtes Backup in einem Profil mit dem smo Backup show Befehl anzeigen.

Mit dem smo Backup show-Befehl werden die folgenden Informationen für jedes Backup angezeigt:

- Die Backup-ID
- Ob die Sicherung erfolgreich war oder fehlgeschlagen ist
- Backup-Umfang (vollständig, teilweise, online oder offline)
- Backup-Modus
- Mount-Status
- Das Backup-Etikett
- Kommentar
- Das Datum und die Uhrzeit, zu der der Vorgang gestartet und beendet wurde
- Informationen darüber, ob das Backup verifiziert wurde
- Die Kategorie für die Aufbewahrung von Backups
- Die Datenbank und der Hostname
- Die Kontrollpunkt-Systemänderungsnummer (SCN)
- Das Ende-Backup-SCN (nur für Online-Backups)
- Die Tabellen und Datendateien der gesicherten Datenbank
- Die Kontrolldateien aus der Datenbank gesichert
- Die Archivprotokolle aus der gesicherten Datenbank
- Das Storage-System und die Volumes, auf denen sich die Dateien befinden
- Die erstellten Snapshot Kopien und deren Speicherort
- Der Status der primären Storage-Ressourcen
- Der Sicherungsstatus
- Backup-Modus

Wenn Sie die Option -wortrecih angeben, werden die folgenden zusätzlichen Informationen angezeigt:

- Die Klone, die aus dem Backup erstellt werden, sofern vorhanden sind
- Verifizierungsinformationen
- Wenn das Backup gemountet ist, zeigt SnapManager die verwendeten Mount-Punkte an

Für die Sicherung der Archivprotokolldatei werden dieselben Informationen angezeigt wie die der anderen Datenbanksicherung, mit Ausnahme der folgenden Informationen:

- Checkpoint SCN
- Backup-SCN beenden
- Tablespace
- Kontrolldateien

Die Sicherung der Archivprotokolldatei enthält jedoch die folgenden zusätzlichen Informationen:

- Die erste Änderungsnummer des Backups
- Die nächste Nummer des Backups
- Thread-Nummer
- Protokoll-ID zurücksetzen
- Inkarnation
- Name der Protokolldatei

a. Geben Sie folgenden Befehl ein:smo Backup show -profileprofile_Name {-labellabel [Data - archivalogs] - id id [-quiet / -verbose]

Verwandte Informationen

Der Befehl smo Backup show

Montage von Backups

SnapManager übernimmt automatisch das Mounten eines Backups, um es dem Host zur Verfügung zu stellen. Sie können Backups auch in Szenarien einbinden, in denen Sie ein externes Tool wie Oracle Recovery Manager (RMAN) für den Zugriff auf die Dateien im Backup verwenden.

Wenn Sie RMAN verwenden, müssen Sie den Mount-Vorgang verwenden, um den Status eines Backups zu ändern (wodurch der Zugriff möglich ist) und den Unmount-Vorgang, um den Status eines Backups zu ändern (wodurch der Zugriff entfernt wird).

Der Befehl smo Backup Mount zeigt eine Liste von Pfaden an, wo die Snapshot Kopien, die aus dem Backup bestehen, gemountet wurden.

Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Backup-Mount-Vorgang sammeln.

1. Geben Sie zum Mounten eines Backups den folgenden Befehl ein: smo Backup Mount -profile profile_Name {labellabel [Data} -archivelogs] [-dump] [-quiet / -verbose]

Verwandte Informationen

Der Befehl smo Backup Mount

UnMounten von Backups

SnapManager hängt automatisch das Backup ab, damit es nicht auf dem Host-Server verfügbar ist. Mit SnapManager können Sie auch die Einbindung aufheben, wenn Sie ein externes Tool wie beispielsweise den Oracle Recovery Manager (RMAN) verwenden, um auf die Dateien im Backup zuzugreifen und den Zustand des Backups zu ändern, um den Zugriff zu entfernen.

Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Unmount-Backup sammeln.

1. Geben Sie folgenden Befehl ein: smo Backup unmount -profile Profile_Name {labellabel [Data} -archivelogs] -idid [-quiet / -verbose] -dump-Force-verbose

Verwandte Informationen

Der Befehl smo Backup unmount

So werden Backups entlastet

Sie können Backups freigeben, die die Snapshot Kopien löschen, ohne die Backup-Metadaten zu löschen. Diese Funktion gibt den Speicherplatz frei, der durch das Backup belegt wird. Sie können den Smo-Backup-freien Befehl verwenden, um die Backups zu befreien.

Damit ein Backup zur Freigabe berechtigt ist, müssen Sie Folgendes sicherstellen:

- Das Backup war erfolgreich
- Backup soll nicht angehängt werden
- Backup verfügt nicht über Klone
- Der Backup darf nicht durch eine Richtlinie zur unbegrenzten Aufbewahrung beibehalten werden
- Das Backup wird nicht bereits freigegeben

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen freien Backup-Vorgang zu sammeln.

1. Geben Sie folgenden Befehl ein: smo Backup free -profilprofile_Name {-labellabel [Data} -archivelogs] [-quiet] [-Force]

Verwandte Informationen

Der smo Backup kostenlose Befehl

Backups werden gelöscht

Sie müssen Backups löschen, wenn Sie sie nicht mehr benötigen. Dadurch wird der Speicherplatz frei, den diese Backups belegen. Wenn Sie Backups entfernen, reduzieren Sie die Wahrscheinlichkeit, dass pro Volume 255 Snapshot Kopien erreicht werden.

- Sie müssen sicherstellen, dass das Backup nicht zum Erstellen eines Klons verwendet wurde.

Sie können Backups, die unbegrenzt aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Optional können Sie die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen Backup-Löschvorgang sammeln.

Wenn Sie die Backups des Archivprotokolls löschen möchten, müssen Sie die für die Sicherung des Archivprotokolls festgelegte Aufbewahrungsdauer überprüfen. Wenn das Backup des Archivprotokolls innerhalb der Aufbewahrungsdauer liegt und die Archivprotokolldateien für die Wiederherstellung einer wiederhergestellten Datenbank erforderlich sind, können Sie das Backup des Archivprotokolls nicht löschen.

1. Überprüfen Sie, ob die Vorgänge abgeschlossen sind, indem Sie den folgenden Befehl eingeben: smo Operationliste -profilprofile_Name-quiet-wortrecih
2. Um ein Backup zu löschen, geben Sie den folgenden Befehl ein:smo Backup delete -profile profile profile Profile_Name [-Label Label [Data - archivalogs] [-idid [-Force] [-dump] [-quiet

   Verwenden Sie die Option -Force, um das Entfernen des Backups zu erzwingen. Wenn Sie das Entfernen eines Backups erzwingen, bei dem unvollständige Vorgänge ausgeführt werden, ist das Backup möglicherweise inkonsistent.

Planen von Datenbank-Backups

Mit SnapManager (3.2 oder höher) für Oracle können Sie Datenbank-Backups regelmäßig während der Stoßzeiten planen, um eine hohe Performance zu gewährleisten. Zum Planen eines Backups können Sie ein Profil erstellen, das die Datenbankinformationen und die Aufbewahrungsrichtlinie enthält, und anschließend die Zeitpläne für das Backup festlegen.

Sie müssen die Backups als Administrator planen. Wenn Sie versuchen, die Backups als nicht vorhandener Benutzer zu planen, zeigt SnapManager eine Fehlermeldung an: Ungültiger Benutzer: Benutzername: Kann keinen Zeitplan-Backup für einen bestimmten Benutzer erstellen

Im Folgenden sind einige planungsbezogene Aufgaben aufgeführt:

- Planen Sie ein Datenbank-Backup auf Stundenbasis, täglich, wöchentlich, monatlich oder einmalig.
- Anzeigen einer Liste geplanter Backups, die einem Profil zugeordnet sind.
- Aktualisierung eines geplanten Backups.
- Einen Zeitplan vorübergehend aussetzen.
- Setzen Sie den angehängten Zeitplan fort.
- Löschen Sie einen Zeitplan.

Das Kontrollkästchen **Jetzt-Menü-Betrieb ausführen** ist deaktiviert, wenn eine geplante Sicherung für diesen Zeitplan ausgeführt wird.

Erstellen von Backup-Zeitplänen

Sie können ein Backup so planen, dass es zu der Zeit und Häufigkeit erfolgt, die für Ihre

Daten und Ihre Umgebung geeignet sind.

Ab SnapManager 3.2 für Oracle können Sie die Backups der Archivprotokolldateien separat planen. Sie müssen jedoch das Profil verwenden, das Sie erstellt haben, um die Archivprotokolldateien zu trennen.

Wenn Sie die Backups der Datendateien und Archivprotokolldateien gleichzeitig geplant haben, erstellt SnapManager zuerst die Datensicherung.

Wenn Sie das Planungsintervall nur als -onetimeonly auswählen, stehen alle Beschneidungsoptionen zur Verfügung. Wenn Sie ein anderes Intervall als nur -onetimeonly auswählen, werden die Beschneidungsoptionen -bis-SCN und -bis-date nicht unterstützt und die folgende Fehlermeldung angezeigt: Die von Ihnen angegebene Option Archivprotokoll pruning, -bis-scn oder -bis-date für das Stundenplanintervall ist ungültig. Geben Sie entweder die Option -ontimeonly für das Planintervall an, oder beschneiden Sie die Archivprotokolle mit einer der Optionen all oder -before {-months} -days/ -weeks -hours.

Wenn in Microsoft Windows Server Failover Cluster (WSFC) und Microsoft Cluster Server (MSCS) Umgebungen ein Failover erfolgt, müssen Sie den SnapManager für Oracle Server neu starten, damit die Service-Adresse (virtuell) dem aktiven Host zugeordnet wird und die SnapManager-Zeitpläne auf den aktiven SnapManager Host angepasst werden.

Wenn in einem anderen Repository derselbe Profil- und Planungsname vorhanden ist, wird der Backup-Planungsvorgang in diesem Repository nicht gestartet. Der Vorgang wird mit der folgenden Meldung beendet: Der Vorgang wird bereits ausgeführt.

1. Geben Sie den folgenden Befehl ein: bbs Schedule create -profile_Name {[-full {-online { -offline}[-contave [-hourly — Weekly — unlimited] [-prove] [-data_pathon2 [files] [-propettaces-pathon2] [-propettaces [-monthly-pathog2] [-pathognoceptaces [-monthly}] [-monthly-pathogloceptaces] [-pathonaces [-pathonaces] [-pathonaces [-}] [-{] [-pathogloceptaces-pathonaces-pathonaces] [-pathonaces-path { -UntilSCN}} -prune -destprune_dest1,prune_dest2] -terminplan-Nameyyy-Schedule_comment] -interval-hourly { -taskrymm -runyytime-time [-choterplan-schedule-schedule_termine] -interval-hourly} {<} -taskrymonthly-user -taskyyyytime [-time]

Ihr Ziel ist	Dann…
Planen Sie eine Sicherung einer Online- oder Offline-Datenbank	Geben Sie -offline oder -online an, um ein Backup der Offline- oder Online-Datenbank zu planen. Wenn Sie diese angeben, können Sie nicht -Auto verwenden.
Lassen Sie SnapManager die Planung einer Datenbank handhaben, unabhängig davon, ob sie online oder offline ist	Angabe -Auto. Wenn Sie „-Auto“ angeben, können Sie „--offline“ oder „-online“ nicht verwenden.
Planen Sie eine Sicherung von Datendateien	Geben Sie -Data -files an, um die durch Kommas getrennten Dateien aufzulisten. Verwenden Sie zum Beispiel die Dateinamen f1,f2,f3.
Planen Sie eine partielle Sicherung bestimmter Tabellen	Legen Sie -Tablespaces fest, um die durch Kommas getrennten Tablespaces aufzulisten. Verwenden Sie zum Beispiel ts1,ts2,ts3.

Planen der Sicherung von Archiv-Log-Dateien	Geben Sie Folgendes an: • -Archivalogs, um die Sicherung der Archivprotokolldateien zu planen • -Backup-dest, um die Ziele für die Archivprotokolldatei zu planen, die in die Sicherung aufgenommen werden sollen • -Exclude-dest, um die Ziele für das Archivprotokoll zu planen, die vom Backup ausgeschlossen werden sollen
Geben Sie die Werte der Aufbewahrungsklasse an	Geben Sie -Retention an und geben Sie an, ob das Backup gemäß einer der folgenden Aufbewahrungsklassen aufbewahrt werden soll: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • -Unbegrenzte SnapManager standardmäßig auf stündlich.
Planen eines Beschneidung von Archivprotokolldateien	Geben Sie Folgendes an: **-Prunelogs, um die Archivprotokolldateien während der Planung eines Backups zu beschneiden** -prune-dest, um das Archivprotokollziel anzugeben, von dem die Archivprotokolldateien beschnitten werden
• Einen Namen für den Terminplan angeben*	Geben Sie -Schedule-Name an.
Sicherung der Datenbank in einem bestimmten Zeitintervall planen	Geben Sie die Option Intervall an und wählen Sie das Zeitintervall aus der folgenden, mit dem die Backups erstellt werden sollen: • -Stündlich • -Täglich • -Wöchentlich • -Monatlich • Nur -ontimeonly

Konfigurieren Sie einen Zeitplan	Geben Sie -cronstring an und enthalten die folgenden sieben Unterausdrücke, die die einzelne Option beschreiben: • 1 bezieht sich auf Sekunden. • 2 bezieht sich auf Minuten. • 3 bezieht sich auf Stunden. • 4 bezieht sich auf einen Tag im Monat. • 5 bezieht sich auf den Monat. • 6 bezieht sich auf einen Tag in einer Woche. • (Optional) 7 bezieht sich auf das Jahr. **Hinweis:** Wenn Sie Ihre Sicherung mit verschiedenen Zeiten in -cronstring und -Start-time geplant haben, dann wird der Zeitplan der Sicherung überschrieben und durch die -Start-Time ausgelöst.
Fügen Sie einen Kommentar zum Backup-Zeitplan	„Specify -terminist-comment“ gefolgt von der Beschreibungstext.
Geben Sie die Startzeit der Zeitplanoperation an	Geben Sie die Startzeit im Format yyyy-mm-dd hh:mm an.
Ändern Sie den Benutzer des geplanten Backup-Vorgangs während der Planung des Backups	Geben Sie -runasuser an. Der Vorgang wird ausgeführt als Benutzer (Root-Benutzer oder Oracle-Benutzer), der den Zeitplan erstellt hat. Sie können jedoch Ihre eigene Benutzer-ID verwenden, wenn Sie gültige Anmeldeinformationen sowohl für das Datenbankprofil als auch für den Host haben.
Aktivieren Sie eine Voraufgabe oder Nachaufgabe des Backup-Zeitplanvorgangs, indem Sie die XML-Datei mit der XML-Datei für die vor- und Nachaufgabe verwenden	Geben Sie die Option -taskSpec an und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation für die Durchführung einer Vorverarbeitung oder einer Nachbearbeitung an, die vor oder nach dem Backup-Zeitplan stattfinden soll.

Aktualisieren eines Backup-Zeitplans

Sie können eine Liste geplanter Vorgänge anzeigen und gegebenenfalls aktualisieren. Sie können die Planungsfrequenz, die Startzeit des Zeitplans, den cronstring-Ausdruck und den Benutzer, der das Backup geplant hat, aktualisieren.

1. Um den Zeitplan für ein Backup zu aktualisieren, geben Sie diesen Befehl ein: smo Schedule Update -profile profile profile_Name-Schedule-nameschedulename [-Schedule-commentplan comment] -interval {-hourly} -Weekly / -monthly / -ontimeonly -Start-timarttime-cronstringcronstring-runasuserrunasuser [-quiet [-verbose]

Anzeigen einer Liste geplanter Vorgänge

Sie können eine Liste der geplanten Vorgänge für ein Profil anzeigen.

1. Um Informationen über den geplanten Vorgang anzuzeigen, geben Sie diesen Befehl ein: smo Schedule list -profile Profile_Name[-quiet / -verbose]

Anhalten von Backup-Zeitplänen

SnapManager ermöglicht Ihnen die Unterbrechung eines Backup-Zeitplans, bis der Backup-Zeitplan wiederaufgenommen wird.

Sie können die aktiven Zeitpläne unterbrechen. Wenn Sie versuchen, den bereits unterbrochenen Backup-Zeitplan zu unterbrechen, wird möglicherweise die Fehlermeldung „Schedule <planename> bereits im Status „suspendieren“ angezeigt.

1. Um den Backup-Zeitplan vorübergehend zu unterbrechen, geben Sie folgenden Befehl ein: smo Schedule suspend -profile_Name-Schedule-nameschedulename [-quiet / -verbose]

Wiederaufnahme der Backup-Pläne

Administratoren haben die Möglichkeit, den angehängten Backup-Zeitplan fortzusetzen.

Wenn Sie versuchen, die aktiven Zeitpläne wieder aufzunehmen, wird möglicherweise die Fehlermeldung „kann nicht fortgesetzt werden: Zeitplan <planename> bereits im Status „fortsetzen“ angezeigt.

1. Um den suspendierten Backup-Zeitplan fortzusetzen, geben Sie diesen Befehl ein: smo Schedule resume -profile Profile_Name-Schedule-nameschedulename [-quiet / -verbose]

Löschen von Backup-Zeitplänen

Sie können Backup-Pläne löschen, wenn diese nicht mehr benötigt werden.

1. Um den Backup-Zeitplan zu löschen, geben Sie folgenden Befehl ein: smo Schedule delete -profile profile_Name-Schedule-nameschedulename [-quiet - verbose]

Datenbank-Backups werden wiederhergestellt

Mit SnapManager für Oracle können Sie eine Datenbank in den Zustand wiederherstellen, an dem sie zum Zeitpunkt der Erstellung einer Snapshot Kopie erstellt wurde. Da Backups häufiger erstellt werden, verringert sich die Anzahl der anzuwendenden Protokolle, sodass die mittlere Zeit bis zur Recovery (MTTR) für eine Datenbank reduziert wird.

Im Folgenden werden einige Aufgaben aufgeführt, die Sie im Zusammenhang mit dem Wiederherstellen und Wiederherstellen von Daten in Datenbanken ausführen können:

- Führen Sie eine dateibasierte Wiederherstellung durch.
- Stellen Sie das gesamte Backup oder einen Teil des Backups wieder her.

  Wenn Sie einen Teil davon wiederherstellen, geben Sie eine Gruppe von Tabellen oder eine Gruppe von

Datendateien an. Sie können auch die Kontrolldateien zusammen mit den Daten oder nur die Kontrolldateien selbst wiederherstellen.

- Stellen Sie die Daten entweder nach einem bestimmten Zeitpunkt oder auf allen verfügbaren Protokollen wieder her, in denen die letzte an die Datenbank verplante Transaktion gespeichert wird.

  Der Zeitpunkt kann eine Oracle System Change Number (SCN) oder ein Datum und eine Uhrzeit (yyyy-mm-dd:hh:mm:ss) sein. Bei SnapManager wird die 24-Stunden-Zeit verwendet.

- Restore aus Backups im Primärspeicher (lokale Backups).
- Stellen Sie das Backup mit SnapManager wieder her, oder verwenden Sie SnapManager für die Wiederherstellung des Backups und verwenden Sie ein anderes Tool wie Recovery Manager (RMAN) zur Wiederherstellung der Daten.
- Wiederherstellung von Backups von alternativen Orten aus

Weitere Informationen finden Sie im *SnapManager for Oracle Best Practices*.

Sie können ein Backup, das von einer früheren Version von SnapManager erstellt wurde, mit SnapManager 3.0 und höher wiederherstellen.

Administratoren können Restore- oder Recovery-Vorgänge über die grafische Benutzeroberfläche von SnapManager oder über die Befehlszeilenschnittstelle (CLI) durchführen.

Verwandte Informationen

Backup von Datenbanken

Der Smo Backup Restore Befehl

"SnapManager for Oracle Best Practices: media.netapp.com/documents/tr-3761.pdf"

Was ist Datenbank-Restore

SnapManager ermöglicht die Durchführung dateibasierter Backup- und Restore-Vorgänge.

In der folgenden Tabelle werden die Wiederherstellungsmethoden beschrieben:

Wiederherstellungsprozess	Details
Dateibasierte Restores	Storage-seitige Wiederherstellung eines vollständigen File-Systems (von primärem oder sekundärem): SnapManager führt eine vollständige Wiederherstellung der Logical Unit Number (LUN) durch.

Storage-seitig komplette Wiederherstellung des Dateisystems

Wenn keine Volume-Wiederherstellung möglich ist, wird ein Storage-seitiges File-System wiederhergestellt, das gesamte File-System kann jedoch auf dem Storage-System wiederhergestellt werden.

Wenn eine Storage-seitige Wiederherstellung eines Dateisystems durchgeführt wird, geschieht Folgendes:

- In einer SAN-Umgebung sind alle vom Filesystem verwendeten LUNs (und ggf. die zugrunde liegende Volume-Gruppe) auf dem Storage-System wiederhergestellt.

Wenn eine Storage-seitige Wiederherstellung des Filesystems erfolgt, hängt vom Speicherort ab:

- Wenn SnapManager aus den primären Storage-Systemen wiederhergestellt wird, sind die LUNs (SAN) vorhanden über SFSR wiederhergestellt.
- Wenn SnapManager aus sekundären Storage-Systemen wiederhergestellt wird, werden die LUNs (SAN) aus sekundären Storage-Systemen über das Netzwerk zurück in das primäre Storage-System kopiert.

Da das Filesystem vollständig wiederhergestellt ist, werden auch Dateien, die nicht zum Backup gehören, zurückgesetzt. Eine Überschreibung ist erforderlich, wenn Dateien, die nicht Teil der Wiederherstellung sind, im Dateisystem vorhanden sind, das wiederhergestellt wird.

Host-seitiges Datei-Restore

Eine Wiederherstellung der Host-seitigen Dateikopien dient als letztes Mittel in SAN-Umgebungen, wenn die Wiederherstellung von Storage-seitigen Dateisystemen und die Wiederherstellung von Dateien auf Storage-Seite nicht durchgeführt werden kann.

Zur Wiederherstellung einer Host-seitigen Dateikopie gehören die folgenden Aufgaben:

- Klonen des Speichers
- Verbinden des geklonten Speichers mit dem Host
- Kopieren von Dateien aus den Klon-Dateisystemen zurück in die aktiven Dateisysteme
- Trennen des Klonspeichers vom Host
- Löschen des Klonspeichers

Backup Recovery

In SnapManager müssen gleichzeitig die Wiederherstellungs- und Recovery-Vorgänge ausgeführt werden. Sie können keinen Wiederherstellungsvorgang ausführen und anschließend einen SnapManager-Wiederherstellungsvorgang später durchführen.

In SnapManager 3.2 oder einer älteren Version können Sie entweder mit SnapManager das Backup wiederherstellen und wiederherstellen, oder mit SnapManager das Backup wiederherstellen und ein anderes Tool wie Oracle Recovery Manager (RMAN) zur Wiederherstellung der Daten verwenden. Da SnapManager die Backups mit RMAN registrieren kann, können Sie die Datenbank mit feineren Besonderheiten wie Blöcken wiederherstellen. Diese Integration vereint die Geschwindigkeit und die Speichereffizienz von Snapshot-Kopien mit der feinen Steuerung für die Wiederherstellung mit RMAN.

Sie müssen eine Datenbank wiederherstellen, bevor Sie sie verwenden können. Sie können jedes beliebige Werkzeug oder Skript verwenden, um eine Datenbank wiederherzustellen.

Ab SnapManager 3.2 für Oracle ermöglicht SnapManager die automatische Wiederherstellung von Datenbank-Backups mithilfe der Archiv-Log-Backups. Selbst wenn die Archiv-Log-Backups am externen Standort zur Verfügung stehen, verwendet SnapManager die Archiv-Log-Backups vom externen Standort zum Wiederherstellen der Datenbank-Backups.

Wenn der Datenbank neue Datendateien hinzugefügt werden, empfiehlt Oracle, sofort ein neues Backup zu erstellen. Wenn Sie außerdem ein Backup wiederherstellen, das vor dem Hinzufügen der neuen Datendateien

erstellt wurde, und versuchen Sie, es nach dem Hinzufügen der neuen Datendateien zu einem Punkt wiederherzustellen, kann der automatische Oracle-Wiederherstellungsprozess fehlschlagen, da es keine Datendateien erstellen kann. In der Oracle-Dokumentation finden Sie Informationen zum Prozess zur Wiederherstellung von Datendateien, die nach einem Backup hinzugefügt wurden.

Für den Wiederherstellungsprozess benötigter Datenbankstatus

Der Status der Datenbank, die wiederhergestellt werden soll, hängt von der Art des Wiederherstellungsprozesses, die Sie durchführen möchten, und der Art der Dateien ab, die enthalten sein sollen.

In der folgenden Tabelle ist der Status aufgeführt, in dem die Datenbank von der ausgewählten Wiederherstellungsoption und dem Typ der Dateien abhängig sein soll, die in die Wiederherstellung aufgenommen werden sollen:

Art der Wiederherstellung	Enthaltene Dateien	Datenbankstatus für diese Instanz
Nur Restore	Kontrolldateien	Herunterfahren
Systemdateien	Montieren oder herunterfahren	Keine Systemdateien
Alle Bundesstaaten	Restore und Recovery	Kontrolldateien
Herunterfahren	Systemdateien	Montieren

Der von SnapManager für einen Wiederherstellungsvorgang erforderliche Datenbankzustand ist von dem ausgeführten Wiederherstellungstyp abhängig (vollständige, partielle oder Kontrolldateien). SnapManager übergibt die Datenbank nicht in einen niedrigeren Zustand (z. B. von Öffnen auf Mount), es sei denn, die Force-Option ist angegeben.

Die Pläne für die Vorschau der Wiederherstellung sind

SnapManager bietet Wiederherstellungspläne vor und nach Abschluss des Wiederherstellungsvorgangs. Mit den Wiederherstellungsplänen werden verschiedene Wiederherstellungsmethoden in der Vorschau, Prüfung und Analyse angezeigt.

Struktur des Wiederherstellungsplans

Der Wiederherstellungsplan besteht aus den folgenden beiden Abschnitten:

- Vorschau/Prüfung: Dieser Abschnitt beschreibt, wie SnapManager jede Datei wiederherstellen (oder wiederherstellen hat).
- Analyse: Dieser Abschnitt beschreibt, warum einige Wiederherstellungsmechanismen während des Wiederherstellungsvorgangs nicht verwendet wurden.

Der Abschnitt Vorschau/Überprüfung

In diesem Abschnitt wird gezeigt, wie jede Datei wiederhergestellt wird oder wiederhergestellt wurde. Wenn Sie den Wiederherstellungsplan vor einem Wiederherstellungsvorgang anzeigen, wird er als Vorschau bezeichnet. Wenn Sie sie nach Abschluss eines Wiederherstellungsvorgangs anzeigen, wird sie als Überprüfung bezeichnet.

Das folgende Vorschaubeispiel zeigt, dass die Dateien mithilfe von speicherseitigen Dateisystemwiederherstellungsmethoden und speicherseitigen Systemwiederherstellungsmethoden wiederhergestellt werden. Um festzustellen, warum alle Dateien nicht mit derselben Wiederherstellungsmethode wiederhergestellt werden würden, lesen Sie den Abschnitt Analyse.

```
Preview:
The following files will be restored completely via: storage side full
file system restore
E:\rac6\sysaux.dbf
E:\rac6\system.dbf
```

Jede Wiederherstellungsmethode hat einen Unterabschnitt, der Informationen über die Dateien enthält, die mit dieser Wiederherstellungsmethode wiederhergestellt werden können. Die Unterabschnitte werden nach abnehmenden Niveaus der Lagermethodeneffizienz geordnet.

Es ist möglich, dass eine Datei durch mehrere Wiederherstellungsmethoden wiederhergestellt werden kann. Mehrere Wiederherstellungsmethoden werden verwendet, wenn die für ein Filesystem verwendeten LUNs (Logical Unit Numbers) auf verschiedene Storage-System-Volumes verteilt werden und einige Volumes für die Volume-Wiederherstellung infrage kommen, andere hingegen nicht. Wenn mehrere Wiederherstellungsmethoden verwendet werden, um dieselbe Datei wiederherzustellen, wird der Vorschaubereich wie folgt angezeigt:

```
The following files will be restored via a combination of:
[storage side file system restore and storage side system restore]
```

Der Abschnitt Analyse

Der Abschnitt Analyse enthält die Gründe, warum einige Wiederherstellungsmechanismen nicht oder wurden nicht verwendet. Anhand dieser Informationen können Sie ermitteln, welche Daten benötigt werden, um effizientere Restore-Mechanismen zu ermöglichen.

Das folgende Beispiel zeigt einen Abschnitt „Analyse“:

```
Analysis:

The following reasons prevent certain files from being
restored completely via: storage side full file system restore
   * LUNs present in snapshot of volume fas960:
        \vol\disks may not be consistent when reverted:
        [fas960:\vol\disks\DG4D1.lun]
     Mapped LUNs in volume fas960:\vol\disks
        not part of the restore scope will be reverted: [DG4D1.lun]

Files to restore:
     E:\disks\sysaux.dbf
     E:\disks\system.dbf
     E:\disks\undotbs1.dbf
     E:\disks\undotbs2.dbf

* Reasons denoted with an asterisk (*) are overridable.
```

Im Beispiel können Sie den ersten Fehler entweder über die Befehlszeilenschnittstelle (CLI) oder durch die Auswahl von **Override** in der grafischen Benutzeroberfläche (GUI) überschreiben. Der zweite Fehler über zugeordnete LUNs im Volume ist obligatorisch und nicht zu überrätselfähig.

Sie können die Prüfungen wie folgt beheben:

- Um einen obligatorischen Prüffehler zu beheben, ändern Sie die Umgebung, damit die Prüfung erfolgreich ist.
- Um einen übersteuerbaren Prüffehler zu beheben, können Sie die Umgebung ändern oder die Prüfung überschreiben.

  Sie müssen jedoch vorsichtig sein, da das Überschreiben der Prüfung zu unerwünschten Folgen führen kann.

Anzeigen der Informationen zur Wiederherstellung von Backups in der Vorschau

Sie können vorab eine Vorschau der Informationen zu einem Backup-Wiederherstellungsprozess anzeigen, um Informationen über die Berechtigung zur Wiederherstellung zu erhalten, die SnapManager für Oracle auf Ihrem Backup gefunden hat. SnapManager analysiert die Daten für Ihr Backup, um festzustellen, ob der Wiederherstellungsprozess erfolgreich abgeschlossen werden kann.

Die Vorschau zur Wiederherstellung enthält die folgenden Informationen:

- Zur Wiederherstellung jeder Datei kann der Wiederherstellungsmechanismus (Storage-seitige Dateisystem-Wiederherstellung, Storage-seitige Datei-Wiederherstellung oder Host-seitige Dateikopie) verwendet werden.
- Warum effizientere Mechanismen nicht für die Wiederherstellung jeder Datei verwendet wurden, wenn Sie die -verbose Option angeben.

Wenn Sie im Befehl Backup Restore die Option-Preview angeben, stellt SnapManager nichts wieder her, listet aber die wiederherzustellenden Dateien auf und gibt an, wie sie wiederhergestellt werden.

Sie können alle Arten von Wiederherstellungsmechanismen in einer Vorschau anzeigen. Die Vorschau zeigt Informationen über bis zu 20 Dateien.

1. Geben Sie den folgenden Befehl ein:smo Backup restore -profileprofile_Name-labellabel-complete -Preview -verbose

   Geben Sie beispielsweise Folgendes ein:

   ```
   smo backup restore -profile targetdb1_prof1
         -label full_bkup_sales_nov_08  -complete -preview -verbose
   ```

   Das folgende Beispiel zeigt die wiederherzustellenden Dateien und listet die verschiedenen Methoden auf, die jeweils verwendet werden:

   ```
   The following files will be restored via storage side full file system
   restore:
   E:\disks\sysaux.dbf
   E:\disks\system.dbf

   The following files will be restored via host side file copy restore:
   E:\disks\undotbs1.dbf
   E:\disks\undotbs2.dbf
   ```

2. Prüfen Sie die Gründe, warum andere Wiederherstellungsprozesse nicht verwendet werden können.
3. Starten Sie den Wiederherstellungsvorgang ohne die Option -Preview, wenn nur Gründe angezeigt werden, die überschreibbar sind.

   Sie können nicht obligatorische Prüfungen weiterhin überschreiben.

Wiederherstellung von Backups auf dem Primärspeicher

Sie können mit dem Befehl Backup Restore ein Datenbank-Backup im Primärspeicher wiederherstellen.

Mithilfe der Befehlsoptionen für die Backup-Wiederherstellung können Sie angeben, ob SnapManager den gesamten oder einen Teil des Backups wiederherstellen soll. Mit SnapManager können Sie außerdem Kontrolldateien zusammen mit den Datendateien oder Tablespaces aus den Backups in einem einzelnen Benutzervorgang wiederherstellen. Sie können -controlfiles mit -Complete integrieren, um Kontrolldateien zusammen mit Tabellen und Datendateien wiederherzustellen.

Sie können eine der folgenden Optionen zur Wiederherstellung des Backups auswählen:

Sie möchten wiederherstellen…	Verwenden…
Das gesamte Backup mit allen Tabellen und Datendateien	-Abgeschlossen
Die Liste bestimmter Tabellen	-Tabellen
Bestimmte Datendateien	-Dateien
Nur die Kontrolldateien	-Controlfiles
Tablespaces, Datendateien und Kontrolldateien	-Complete -controlfiles

Sie können das Backup auch von einem alternativen Speicherort wiederherstellen, indem Sie -restorespec angeben.

Wenn Sie -Recovery einschließen, können Sie die Datenbank wiederherstellen, um:

- Zur letzten Transaktion, die in der Datenbank durchgeführt wurde (alle Logs)
- Zu einem bestimmten Datum und einer bestimmten Uhrzeit
- Eine bestimmte Oracle Systemänderungsnummer (SCN)
- Zum Zeitpunkt des Backups (keine Protokolle)
- Nur Restore

Sowohl die Datums- als auch die Zeitwiederherstellung sowie die SCN-Wiederherstellung sind Point-in-Time Recovery.

SnapManager (3.2 oder höher) bietet die Möglichkeit, die wiederhergestellten Datenbank-Backups automatisch mithilfe der Archivprotokolldateien wiederherzustellen. Selbst wenn die Archivprotokolldateien am externen Speicherort verfügbar sind, wenn Sie die Option -recover-from-location angeben, verwendet SnapManager die Archivprotokolldateien vom externen Speicherort, um die wiederhergestellten Datenbank-Backups wiederherzustellen.

Wenn Sie die externen Archivprotokolle für die Wiederherstellung der wiederhergestellten Backups angeben, müssen Sie sicherstellen, dass Sie die externen Standortnamen in Großbuchstaben eingeben. Im Dateisystem müssen sich alle Ordner- und Unterordner-Namen in Großbuchstaben befinden, da Oracle den Zielpfad in Großbuchstaben übersetzt und erwartet, dass die externen Zielpfade, Ordnernamen und Unterordnernamen in Großbuchstaben enthalten sind. Wenn Sie die Pfade für das externe Archivprotokoll in Kleinbuchstaben angeben, kann Oracle den angegebenen Pfad möglicherweise nicht identifizieren und kann die Datenbank nicht wiederherstellen.

SnapManager stellt Oracle den externen Standort zur Verfügung. Aber Oracle erkennt die Dateien vom externen Ziel nicht. Dieses Verhalten wird beim Ziel des Flash-Recovery-Bereichs bemerkt. Dies sind Probleme mit Oracle und die Problemumgehung besteht darin, immer eine Sicherung von Archiv-Log-Dateien in solchen Datenbank-Layouts zu haben.

Wenn ein inkonsistentes SCN oder Datum angegeben wird, wird die Wiederherstellung am letzten konsistenten Punkt, der mit der Fehlermeldung Wiederherstellung erfolgreich, aber nicht ausreichend beendet. Die Wiederherstellung muss manuell in einen konsistenten Zustand erfolgen.

Für eine Wiederherstellung, wenn keine Protokolle angewendet werden, stellt SnapManager bis zum letzten SCN der letzten während des Backups erstellten Archivprotokolldatei wieder her. Wenn die Datenbank konsistent ist bis zu diesem SCN, dann wird die Datenbank erfolgreich geöffnet. Wenn die Datenbank zu diesem Zeitpunkt nicht konsistent ist, versucht SnapManager immer noch, die Datenbank zu öffnen, die erfolgreich geöffnet wird, wenn die Datenbank bereits konsistent ist.

SnapManager unterstützt nicht die Wiederherstellung der ausschließlich Archiv-Log-Backups.

Wenn das Archivprotokoll-Ziel kein Snapshot-fähiger Storage ist, können Sie mit SnapManager die wiederhergestellten Datenbank-Backups mithilfe des Profils wiederherstellen. Bevor Sie SnapManager-Vorgänge auf einem nicht-Snapshot-fähigen Storage durchführen, sollten Sie die Ziele für archivedLogs.exclude in smo.config hinzufügen.

Sie müssen sicherstellen, dass Sie den Parameter Ausschließen festlegen, bevor Sie ein Profil erstellen. Erst nachdem der Parameter exclude in der SnapManager-Konfigurationsdatei festgelegt wurde, ist die Profilerstellung erfolgreich.

Wenn das Backup bereits angehängt ist, mounted SnapManager den Backup nicht erneut und verwendet das bereits bereitgestellte Backup. Wenn das Backup von einem anderen Benutzer gemountet wird und der aktuelle Benutzer keinen Zugriff auf das zuvor bereitgestellte Backup hat, müssen andere Benutzer die Berechtigungen bereitstellen. Alle Archivprotokolldateien haben Leseberechtigungen für die Gruppen-Eigentümer; der aktuelle Benutzer hat möglicherweise nicht die Berechtigungen, wenn das Backup von einer anderen Benutzergruppe gemountet wird. Die Benutzer können Berechtigungen für die gemounteten Archivprotokolldateien manuell erteilen und die Wiederherstellung oder Wiederherstellung wiederholen.

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen Wiederherstellungsvorgang zu sammeln.

1. Geben Sie den folgenden Befehl ein:smo Backup restore -profile_Name-Label-complete-recover -alllogs [-recover-from-locationpath [,path2]]-dump-verbose

   smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 - complete -restore -alllogs -wortrecih

2. Um Daten für verschiedene Szenarien wiederherzustellen, führen Sie einen der folgenden Schritte aus:

Sie möchten wiederherstellen…	Befehlsbeispiel
Vollständige Datenbank ohne Kontrolldateien und Wiederherstellung auf eine bestimmte SCN-Nummer (3794392). In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber alle Datendateien sind beschädigt oder verloren. Stellen Sie die Datenbank von einem bestehenden vollständigen Online-Backup auf einen Punkt unmittelbar vor diesem SCN. wieder her	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -Recovery -bis 3794392 -verbose
Komplette Datenbank ohne Kontrolldateien und Wiederherstellung bis zu einem Datum und einer Uhrzeit.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -Recovery -until 2008-09-15:15:29:23 -verbose

Sie möchten wiederherstellen…	Befehlsbeispiel
Komplette Datenbank ohne Kontrolldateien und Wiederherstellung bis zu einer Daten und Zeit. In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber alle Datendateien sind beschädigt oder verloren oder ein logischer Fehler trat nach einer bestimmten Zeit auf. Stellen Sie die Datenbank von einem bestehenden kompletten Online-Backup auf ein Datum und eine Uhrzeit unmittelbar vor dem Fehlerpunkt wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -Recovery -bis „2008-09-15:15:29:23“ -verbose
Partielle Datenbank (eine oder mehrere Datendateien) ohne Kontrolldateien und wiederherstellen mit allen verfügbaren Protokollen. In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber eine oder mehrere Datendateien sind beschädigt oder verloren. Stellen Sie diese Dateien wieder her und stellen Sie die Datenbank von einem bestehenden vollständigen Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -Files E:\Disks\s02.dbf E:\Disks\sales03.dbf E:\Disks\sale04.dbf -Recovery -alllogs -verbose
Partielle Datenbank (ein oder mehrere Tabellen) ohne Kontrolldateien und Recovery mit allen verfügbaren Protokollen. In diesem Fall sind die aktuellen Steuerdateien vorhanden, aber ein oder mehrere Tabellen werden verworfen oder eine von mehreren Datendateien, die zu dem Tablespace gehören, ist beschädigt oder verloren. Stellen Sie diese Tabellen wieder her und stellen Sie die Datenbank aus einem vorhandenen kompletten Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -Tablespaces Users -Recovery -alllogs -verbose
Nur Steuern Dateien und erholen mit allen verfügbaren Protokollen. In diesem Fall existieren die Datendateien, aber alle Kontrolldateien sind beschädigt oder verloren. Stellen Sie nur die Steuerdateien wieder her und stellen Sie die Datenbank aus einem bestehenden vollständigen Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -controlfiles -Recovery -alllogs -verbose

Sie möchten wiederherstellen…	Befehlsbeispiel
Vollständige Datenbank ohne Kontrolldateien und Wiederherstellung mit den Backup-Kontrolldateien und allen verfügbaren Protokollen. In diesem Fall sind alle Datendateien beschädigt oder verloren gegangen. Stellen Sie nur die Steuerdateien wieder her und stellen Sie die Datenbank aus einem bestehenden vollständigen Online-Backup mit allen verfügbaren Protokollen wieder her.	smo Backup Restore -profile targetdb1_Prof1 -Label full_bkup_Sales_nov_08 -complete -using-Backup -controlfile -recover -alllogs -wortrecih
Wiederherstellen der wiederhergestellten Datenbank mit den Archiv-Log-Dateien aus dem externen Archiv-Log-Speicherort.	smo Backup Restore -profile targetdb1_prog1 -Label full_bkup_Sales_nov_08 -complete -using -Backup-controlfile -recover -alllogs -recover-from -location E:\Archive -verbose

3. Geben Sie mithilfe der Option -recover-from-location externe Archivprotokolle an.

Verwandte Informationen

Wiederherstellen von Backups von einem alternativen Speicherort

Der Smo Backup Restore Befehl

Durchführen von Recovery auf Blockebene mit Oracle Recovery Manager (RMAN)

Sie können SnapManager für den Katalog seiner Backups im Recovery Manager (RMAN), einem Oracle Tool, konfigurieren, damit Sie mithilfe von RMAN ein Recovery auf Blockebene durchführen können. RMAN kann die Kontrolldateien der Datenbank oder eine separate Recovery-Katalog-Datenbank als Repository verwenden.

1. Geben Sie den folgenden Befehl ein, um eine vollständige Offline-Sicherung mithilfe von SnapManager durchzuführen:

   smo Backup create -offline-full-profilprofile_Name-labelBackup_Label_Name-wortrecih

   Wo?

   - Profile_Name ist der Name des Profils, das der Sicherung zugeordnet ist
   - Backup_Label_Name ist der Name des Backup-Labels

```
smo backup create -offline -full -profile profile_monthly
-label full_backup -verbose

+
SMO-07109 [INFO ]: Cataloguing all files in backup set with RMAN
TAG=SMC_full_backup_1158773581857, RMAN=ES0/controlfile.
...
SMO-13037 [INFO ]: Successfully completed operation: Backup
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:02:20.506
Operation Id [ff8080810dcc47e3010dcc47eb7a0001] succeeded.
+
```

1. Um zu überprüfen, ob das Backup mit RMAN katalogisiert ist, geben Sie vom Datenbank-Host den folgenden Befehl an der RMAN-Eingabeaufforderung ein:

   Liste datafilecopy Tag Tag Tag_Name;

2. Geben Sie den folgenden Befehl ein, um die Datenbank zu überprüfen und festzustellen, ob Blöcke beschädigt sind:

   dbv-DATEI=user01.dbf

   Die folgende Ausgabe gibt an, dass zwei Seiten beschädigt sind:

```
DBVERIFY: Release 10.2.0.1.0 - Production on Wed Sep 20 13:35:44 2006
Copyright (c) 1982, 2005, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = user01.dbf
Page 625 is marked corrupt
Corrupt block relative dba: 0x01400271 (file 5, block 625)
Bad header found during dbv:
Data in bad block:
type: 240 format: 6 rdba: 0xed323b81
last change scn: 0x6f07.faa74628 seq: 0x87 flg: 0x02
spare1: 0x60 spare2: 0x5 spare3: 0xef7d
consistency value in tail: 0xa210fe71
check value in block header: 0x13c7
block checksum disabled...
Page 627 is marked corrupt
Corrupt block relative dba: 0x01400273 (file 5, block 627)
Bad header found during dbv:
Data in bad block:
type: 158 format: 7 rdba: 0x2101e16d
last change scn: 0xe828.42414628 seq: 0xb4 flg: 0xff
spare1: 0xcc spare2: 0x81 spare3: 0x8665
consistency value in tail: 0x46d20601
check value in block header: 0x1a84
computed block checksum: 0x6c30
DBVERIFY - Verification complete
Total Pages Examined : 1280
Total Pages Processed (Data) : 1123
Total Pages Failing (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing (Index): 0
Total Pages Processed (Other): 34
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
Total Pages Empty : 120
Total Pages Marked Corrupt: 2
Total Pages Influx : 0
Highest block SCN : 1337349 (0.1337349)
```

3. Um den Zugriff auf die Dateien vom Backup auf den Host und RMAN zu ermöglichen, mounten Sie das Backup mit dem folgenden Befehl:

   smo Backup Mount -profileprofile_Name-labellabel-verbose

```
smo backup mount -profile SALES1 -label full_backup -verbose

SMO-13046 [INFO ]: Operation GUID 8abc013111b9088e0111b908a7560001
starting on Profile SALES1
SMO-08052 [INFO ]: Beginning to connect mount(s) [E:\logs,F:\data] from
logical snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001.
SMO-08025 [INFO ]: Beginning to connect mount E:\logs from snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_logs.
SMO-08027 [INFO ]: Finished connecting mount E:\logs from snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_logs.
SMO-08025 [INFO ]: Beginning to connect mount F:\data from snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_data.
SMO-08027 [INFO ]: Finished connecting mount F:\data from snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001_0 of volume
hs_data.
SMO-08053 [INFO ]: Finished connecting mount(s) [E:\logs,F:\data] from
logical snapshot
SMO_SALES1_hsdb1_F_C_1_8abc013111a450480111a45066210001.
SMO-13037 [INFO ]: Successfully completed operation: Backup Mount
SMO-13048 [INFO ]: Operation Status: SUCCESS
SMO-13049 [INFO ]: Elapsed Time: 0:01:00.981
Operation Id [8abc013111b9088e0111b908a7560001] succeeded.
```

4. Geben Sie zum Wiederherstellen der Blöcke in RMAN den folgenden Befehl ein:

   Blockrecover-Datendatei 'E:\path\file.dbf' Block Block_id, from Tag Backup_rman_Tag

```
RMAN> blockrecover datafile
'E:\sys\file01.dbf' block 625, 626, 627
from tag SMO_full_backup_1158773581857;

Starting blockrecover at 20-SEP-08 using target database control file
instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=153 devtype=DISK
channel ORA_DISK_1: restoring block(s) from datafile copy
 C:\myfs\user01.dbf
starting media recovery
media recovery complete, elapsed time: 00:00:01
Finished blockrecover at 20-SEP-08
```

5. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die Blöcke repariert wurden:

   dbv-DATEI=filename.dbf

   Die folgende Ausgabe zeigt an, dass keine Seiten beschädigt sind:

```
dbv FILE=user01.dbf

DBVERIFY: Release 10.2.0.1.0 - Production on Wed Sep 20 13:40:01 2008
Copyright (c) 1982, 2008, Oracle. All rights reserved.
DBVERIFY - Verification starting : FILE = user01.dbf
DBVERIFY - Verification complete
Total Pages Examined : 1280
Total Pages Processed (Data) : 1126
Total Pages Failing (Data) : 0
Total Pages Processed (Index): 0
Total Pages Failing (Index): 0
Total Pages Processed (Other): 34
Total Pages Processed (Seg) : 0
Total Pages Failing (Seg) : 0
Total Pages Empty : 120
Total Pages Marked Corrupt : 0
Total Pages Influx : 0
Highest block SCN : 1337349 (0.1337349)
```

   Alle beschädigten Blöcke wurden repariert und wiederhergestellt.

Wiederherstellung von Dateien aus einem anderen Speicherort

SnapManager ermöglicht Ihnen, Datendateien von einem anderen Speicherort als die von Snapshot Kopien im ursprünglichen Volume wiederherzustellen und zu kontrollieren.

Der ursprüngliche Speicherort ist der Speicherort der Datei auf dem aktiven Dateisystem zum Zeitpunkt des Backups. Der alternative Speicherort ist der Speicherort, von dem eine Datei wiederhergestellt wird.

Sie können die Datendateien von einem alternativen Speicherort wiederherstellen, um sie von einem Zwischendateisystem in ein aktives Dateisystem wiederherzustellen.

Die Recovery wird durch SnapManager automatisiert. Bei der Wiederherstellung von Dateien von externen Speicherorten verwendet SnapManager den Befehl „Wiederherstellung automatisch von Standort aus“.

SnapManager setzt für die Wiederherstellung von Dateien auch den Oracle Recovery Manager (RMAN) ein. Die wiederherzustellenden Dateien sollten von Oracle erkennbar sein. Die Dateinamen sollten im Standardformat vorliegen. Bei der Wiederherstellung aus einem Flash-Recovery-Bereich liefert SnapManager den übersetzten Weg zu Oracle. Oracle ist jedoch nicht aus dem Flash-Recovery-Bereich wiederhergestellt, da es nicht den richtigen Dateinamen generieren kann. Idealerweise sollte der Flash-Recovery-Bereich als Ziel mit RMAN genutzt werden.

Verwandte Informationen

Stellen Sie Backups aus einer Übersicht über einen alternativen Speicherort wieder her

Verwenden Sie zum Wiederherstellen eines Datenbank-Backups von einem anderen Standort die folgenden wichtigen Schritte, die jeweils weiter in diesem Abschnitt beschrieben werden.

- Führen Sie je nach Datenbank-Layout einen der folgenden Schritte aus:
  - Stellen Sie die erforderlichen Datendateien von Band, SnapVault, SnapMirror oder anderen Medien auf jedem beliebigen Filesystem wieder her, das auf dem Datenbank-Host gemountet ist.
  - Stellen Sie das erforderliche Dateisystem wieder her und mounten Sie es auf dem Datenbank-Host.
  - Stellen Sie eine Verbindung zu den erforderlichen RAW-Geräten her, die im lokalen Host vorhanden sind.
- Erstellen Sie eine XML-Datei (Extensible Markup Language) für die Wiederherstellungsspezifikation, die die Zuordnungen enthält, die SnapManager vom alternativen Speicherort zum ursprünglichen Speicherort wiederherstellen muss. Speichern Sie die Datei an einem Speicherort, auf den SnapManager zugreifen kann.
- Verwenden Sie SnapManager, um die Daten mithilfe der XML-Datei für die Wiederherstellungsspezifikation wiederherzustellen und wiederherzustellen.

Wiederherstellung der Daten aus Dateien

Bevor Sie ein Restore von einem alternativen Speicherort aus durchführen, müssen Sie die erforderlichen Dateien von einem beliebigen Storage-Medium wiederherstellen und die Dateien von Applikationen wie SnapVault oder SnapMirror in einem Dateisystem wiederherstellen, das auf dem lokalen Host gemountet ist.

Sie können die Wiederherstellung aus einem alternativen Speicherort verwenden, um die Dateien von einem alternativen Dateisystem auf ein aktives Dateisystem zu kopieren.

Sie müssen die alternativen Speicherorte angeben, von denen die Originaldateien wiederhergestellt werden sollen, indem Sie eine Wiederherstellungsspezifikation erstellen.

Wiederherstellung von Daten aus dem Dateisystem

Bevor Sie Daten von einem alternativen Speicherort wiederherstellen, müssen Sie das erforderliche Filesystem wiederherstellen und es auf dem lokalen Host mounten.

Sie können den Wiederherstellungsvorgang von einem alternativen Speicherort aufrufen, um die Dateien von alternativen Dateisystemen auf aktive Dateisysteme zu kopieren.

Um diesen Vorgang durchzuführen, müssen Sie die alternativen Mount-Punkte angeben, von denen die ursprünglichen Mount-Punkte und die Namen der ursprünglichen Snapshot-Kopie wiederhergestellt werden sollen, indem Sie eine Spezifikationsdatei für die Wiederherstellung erstellen.

Der Name der Snapshot Kopie ist eine erforderliche Komponente, da dasselbe Filesystem mehrmals in einer einzelnen Backup-Operation gesichert werden kann (z. B. einmal für die Datendateien und einmal für die Log-Datei).

Verwandte Informationen

Erstellen von Wiederherstellungsspezifikationen

Erstellen von Wiederherstellungsspezifikationen

Die Spezifikationsdatei für die Wiederherstellung ist eine XML-Datei, die die ursprünglichen und alternativen Speicherorte enthält, aus denen die Datei wiederhergestellt werden kann. SnapManager verwendet diese Spezifikationsdatei, um Dateien vom angegebenen Speicherort wiederherzustellen.

Sie können die Wiederherstellungsspezifikationsdatei mit einem beliebigen Texteditor erstellen. Sie müssen eine .XML-Erweiterung für die Datei verwenden.

1. Öffnen Sie eine Textdatei.
2. Geben Sie Folgendes ein: <restore-Specification xmlns="" class="bare">http://www.netapp.com">
3. Geben Sie alle Informationen zur Dateizuordnung unter Verwendung des im folgenden Beispiel gezeigten Formats ein:

```
<file-mapping>
    <original-location>E:\disks\sysaux.dbf</original-location>
    <alternate-location>E:\disks\sysaux.dbf</alternate-location>
</file-mapping>
```

   Die Dateizuordnung gibt an, aus welcher Datei wiederhergestellt wird. Der ursprüngliche Speicherort ist der Speicherort der Datei auf dem aktiven Dateisystem zum Zeitpunkt der Sicherung. Der alternative Speicherort ist der Speicherort, von dem die Datei wiederhergestellt wird.

4. Geben Sie alle Informationen zur Dateisystemzuordnung unter Verwendung des im Beispiel gezeigten Formats ein:

```
<mountpoint-mapping>
     <original-location>E:\disks\sysaux.dbf</original-location>
     <snapname>snapname</snapname>
     <alternate-location>E:\disks\sysaux.dbf</alternate-location>
</mountpoint-mapping>
```

   Mountpunkt bezieht sich auf Verzeichnispfad C:\myfs. Die Mountpunkt-Mapping-Zuordnung gibt den Bereitstellungspunkt an, aus dem die Dateien wiederhergestellt werden. Der ursprüngliche Speicherort ist der Speicherort des Mountpoint im aktiven File-System zum Zeitpunkt des Backups. Der alternative Speicherort ist der Bereitstellungspunkt, aus dem die Dateien im ursprünglichen Speicherort wiederhergestellt werden. Der Snapname ist der Name der Snapshot Kopie, in der die Originaldateien gesichert wurden.

   > Der Name einer Snapshot Kopie ist eine notwendige Komponente, da dasselbe Filesystem in einem einzelnen Backup-Vorgang mehrfach eingesetzt werden kann (z. B. einmal für die Datendateien und einmal für die Protokolle).

5. Geben Sie Folgendes ein: </Restore-Specification>
6. Speichern Sie die Datei als .XML-Datei und schließen Sie die Spezifikation.

Wiederherstellen von Backups von einem alternativen Speicherort

Sie können die Datendateien von einem alternativen Speicherort wiederherstellen, um sie von einem Zwischendateisystem in ein aktives Dateisystem wiederherzustellen.

- Erstellen Sie eine XML-Datei für die Wiederherstellungsspezifikation, und geben Sie den Typ der Wiederherstellungsmethode an, die Sie verwenden möchten.

Sie können den Befehl smo Backup restore verwenden und die XML-Datei für die Wiederherstellungsspezifikation angeben, die Sie erstellt haben, um das Backup von einem anderen Speicherort wiederherzustellen.

1. Geben Sie den folgenden Befehl ein: smo Backup restore -profilprofile-labellabel-complete-alllogs -restorespecrestorespec

Verwandte Informationen

Der Smo Backup Restore Befehl

Klonen der Datenbank-Backup

Wenn Sie eine Datenbank klonen, können Sie Aufgaben wie das Testen eines Upgrades auf eine Datenbank durchführen, ohne die produktive Datenbank zu beeinträchtigen, eine Master-Installation auf mehrere Trainingssysteme zu duplizieren oder eine Master-Installation als Basisinstallation auf andere Server mit ähnlichen Anforderungen zu duplizieren.

Sie können die folgenden Aufgaben zum Klonen ausführen:

- Klonen einer Datenbank aus einem vorhandenen Backup
- Klonen einer Datenbank im aktuellen Status, mit der Sie das Backup und den Klon in einem Verfahren erstellen können.
- Klonen Sie eine Datenbank und verwenden Sie benutzerdefinierte Plug-in-Skripte, die vor oder nach dem Klonvorgang ausgeführt werden.
- Klonen einer Datenbank auf demselben Host, auf dem sich die Datenbank befindet.
- Klonen einer Datenbank unter Verwendung von Archivprotokolldateien aus dem externen Archivprotokoll.
- Klonen einer Datenbank auf einem alternativen Host
- Zeigen Sie eine Liste von Klonen an.
- Anzeigen von detaillierten Kloninformationen
- Klone löschen

Klonen

Sie können eine Datenbank klonen, um ein exaktes Replikat der Originaldatenbank zu erstellen. Sie können den Klon von einem vollständigen Backup oder vom aktuellen

Status der Datenbank aus erstellen.

Zum Erstellen eines Klons mit SnapManager gehören folgende Vorteile:

Vorteile	Details
Schnell	Der Klonvorgang bei SnapManager nutzt die in Data ONTAP verfügbare FlexClone Funktion. Somit können Sie große Datenvolumen schnell klonen.
Platzeffizienz	Wenn Sie einen Klon mit SnapManager erstellen, wird Speicherplatz nur für die Änderungen zwischen dem Backup und dem Klon benötigt. Ein SnapManager-Klon ist eine beschreibbare Snapshot Kopie der Originaldatenbank und kann nach Bedarf erweitert werden. Hingegen erfordert ein physischer Klon der Datenbank, dass Ihnen genügend Speicherplatz zum Kopieren der gesamten Datenbank zur Verfügung steht.
Virtuelle Kopie	Sie können die geklonte Datenbank so verwenden, als wäre sie die ursprüngliche Datenbank. Beispielsweise können Sie einen Klon für Tests, Überprüfungen von Plattformen und Updates, Mehrfachsimulationen mit großen Datenmengen und Tests und Probeläufe an Remote Standorten verwenden. Änderungen am Klon haben keine Auswirkung auf die ursprüngliche Datenbank. Nachdem die Datenbank geklont wurde, ist die geklonte Datenbank vollständig betriebsbereit.
Einfachheit	Sie können eine Datenbank mithilfe von SnapManager Befehlen auf einem beliebigen Host klonen.

Sie müssen sicherstellen, dass die folgenden Voraussetzungen erfüllt sind, bevor eine Datenbank geklont werden kann:

- Löschen Sie die Datei sfile<SID>.ora aus €€Oracle_HOME\Datenbank.
- Löschen Sie die Datei init<SID>.ora aus €€Oracle_HOME\Datenbank.
- Löschen Sie die Oracle Dump-Ziele, die in der Klon-Spezifikations-Datei angegeben sind.
- Löschen Sie die Oracle-Steuerdateien, die in der Klon-Spezifikations-Datei angegeben sind.
- Löschen Sie die Oracle Redo-Protokolldateien, die in der Klon-Spezifikations-Datei angegeben sind.

Sie müssen dem Klon eine neue Systemkennung geben. Sie können nicht gleichzeitig zwei Datenbanken mit derselben Systemkennung auf demselben Host ausführen. Sie können einen Klon auf einem anderen Host mit der gleichen Systemkennung erstellen. Sie können den Klon entweder mit einer Bezeichnung versehen oder SnapManager eine Bezeichnung erstellen lassen. Dazu verwenden Sie die Systemkennung, das Datum und die Uhrzeit der Klonerstellung.

Wenn Sie ein Etikett eingeben, dürfen Sie keine Leerzeichen oder Sonderzeichen enthalten.

Im Rahmen des Klonprozesses erstellt SnapManager die nötigen Oracle Dateien und Parameter für die geklonte Datenbank. Ein Beispiel für eine notwendige Oracle-Datei ist init<SID>.ora.

Wenn Sie eine Datenbank klonen, erstellt SnapManager eine neue init<SID>.ora-Datei für die Datenbank im Verzeichnis Oracle_HOME\.

Wenn SnapManager den Storage für eine Datenbank klonen, erstellt es auch einen neuen Filesystem-Bereitstellungspunkt, ändert aber nicht die Verzeichnisstruktur unter dem Bereitstellungspunkt aus der SnapManager CLI. In der SnapManager GUI können Sie jedoch die Verzeichnisstruktur und die Metadaten des Dateisystems ändern.

Sie können ein Datenbank-Backup auf dem Host, auf dem sich die Datenbank befindet, oder auf einem alternativen Host klonen.

Wenn die geklonte Datenbank eine spfile verwendet, erstellt SnapManager eine spfile für den Klon. Diese Datei wird in das Datenbankverzeichnis €Oracle_HOME\gespeichert und erstellt die Verzeichnisstruktur für die Diagnosedateien. Der Dateiname ist sfile <SID>.ora.

Klonmethoden

Sie können eine Datenbank mit einer von zwei Methoden klonen. Die von Ihnen gewählte Methode wirkt sich auf den Erstellungsvorgang des Klons aus.

In der folgenden Tabelle werden die Klonmethoden und ihre Auswirkung auf den Vorgang zum Erstellen von Klonen und seine Option -Reserve beschrieben. Eine LUN kann mit beiden Methoden geklont werden.

Klonmethode
Beschreibung
Clone create -Reserve
Klonen von LUNs
Es wird eine neue Klon-LUN innerhalb desselben Volumes erstellt.
Wenn -Reserve für eine LUN auf „yes“ eingestellt ist, ist der Speicherplatz für die volle LUN-Größe innerhalb des Volume reserviert.
Klonen von Volumes
Es wird ein neuer FlexClone erstellt und die Klon-LUN innerhalb des neuen Klon-Volume vorhanden ist. Verwendet FlexClone Technologie.
Wenn -Reserve für ein Volume auf „ja“ eingestellt ist, ist der Speicherplatz für die volle Volume-Größe innerhalb des Aggregats reserviert.

Erstellen von Klonspezifikationen

SnapManager für Oracle verwendet eine XML-Datei für die Klonspezifikation, die die Zuordnungen, Optionen und Parameter für die Verwendung im Klonvorgang umfasst.

SnapManager verwendet diese Informationen, um zu bestimmen, wo die von ihm klonen und wie mit Diagnosedaten, Kontrolldateien, Parametern usw. umzugehen ist.

Sie können die Klon-Spezifikationsdatei über die grafische Benutzeroberfläche von SnapManager (GUI), die Befehlszeilenschnittstelle (CLI) oder einen Texteditor erstellen.

Wenn Sie die Clone Specification-Datei mithilfe eines Texteditors erstellen, müssen Sie sie als XML-Datei speichern. Sie können diese XML-Datei für andere Klonvorgänge verwenden.

Sie können auch eine Vorlage für Klonspezifikationen erstellen und diese dann anpassen. Sie können den Befehl „smo Clone template“ oder in der GUI verwenden, den Clone Wizard verwenden.

SnapManager für Oracle fügt einer beliebigen Klon-Spezifikations-Vorlage, die sie erstellt, einen Versionsstring hinzu. SnapManager für Oracle geht von der neuesten Version für jede Klon-Spezifikations-Datei aus, die keinen Versionsstring enthält.

Wenn Sie Remote-Klone durchführen möchten, ändern Sie in der Klonspezifikationsdatei nicht die Standardorte der Datendateien, Wiederherstellungsprotokolle und Kontrolldateien. Wenn Sie den Standardspeicherort ändern, erstellt SnapManager nicht den Klon oder erstellt den Klon für einer Datenbank, die keine Snapshot-Funktion unterstützt. Daher schlägt die automatische Profilerstellung fehl.

Obwohl Mount-Punkt- und ASM-Datenträgergruppen-Informationen über die GUI editierbar sind, können Sie nur den Dateinamen und nicht die Dateiorte ändern.

Sie können eine Aufgabe mehrfach ausführen, entweder mit den gleichen oder mit unterschiedlichen Parameter- und Wertkombinationen.

1. Öffnen Sie eine Textdatei und geben Sie Text ein, wie im folgenden Beispiel gezeigt:

```
<clone-specification xmlns="http://www.example.com>
     <storage-specification/>
     <database-specification/>
 </clone-specification>
```

2. Geben Sie in der Komponente Speicherspezifikation die Bereitstellungspunkte für die Datendateien ein.

   In der Storage-Spezifikation werden die Speicherorte für den für den Klon erstellten neuen Storage aufgeführt, wie z. B. Mount-Punkte für Datendateien und Rohgeräte. Diese Elemente müssen vom Quell- dem Ziel zugeordnet werden.

   Im folgenden Beispiel wird die Syntax für den Mount-Punkt der Datendatei angezeigt, die Sie in der Klonspezifikation verwenden:

```
<mountpoint>
     <source>\mnt\path\source_data file_mountpoint</source>
     <destination>\mnt\path\target_data file_mountpoint</destination>
</mountpoint>
```

3. Geben Sie in der Komponente Datenbankspezifikation die Informationen der Steuerdatei als eine Liste der Steuerdateien an, die Sie für den Klon erstellen möchten.

Die Datenbankspezifikation gibt die Datenbankoptionen für den Klon an, z. B. Kontrolldateien, Wiederherstellungsprotokolle, Archivprotokolle und Oracle Parameter.

Im folgenden Beispiel wird die Syntax der Kontrolldatei angezeigt, die Sie in der Klonspezifikation verwenden:

```
<controlfiles>
     <file>\mnt\path\clonename\control\control01.ctl</file>
     <file>\mnt\path\clonename\control\control02.ctl</file>
</controlfiles>
```

4. Geben Sie die Struktur des Wiederherstellungsprotokolls für den Klon an.

   Im folgenden Beispiel wird die Struktur des Wiederherstellungsprotokollverzeichnisses für das Klonen angezeigt:

```
<redologs>
     <redogroup>
          <file>\mnt\path\clonename\redo\redo01.log</file>
          <number>1</number>
          <size unit="M">100</size>
     </redogroup>
     <redogroup>
         <file>\mnt\path\clonename\redo\redo02.log</file>
         <number>2</number>
         <size unit="M">100</size>
     </redogroup>
</redologs>
```

5. Geben Sie die Oracle-Parameter an, die in der geklonten Datenbank auf unterschiedliche Werte festgelegt werden sollen. Wenn Sie Oracle 10 verwenden, müssen Sie die folgenden Parameter angeben:
   - Hintergrundauszug
   - Core Dump
   - User Dump
   - (Optional) Archivprotokolle

   > Wenn die Parameterwerte nicht richtig festgelegt sind, wird der Klonvorgang angehalten, und Sie erhalten eine Fehlermeldung.

   Wenn Sie nicht den Speicherort der Archivprotokolle angeben, erstellt SnapManager den Klon im Noarchivelog Modus. SnapManager kopiert diese Parameterinformationen in die init.ora-Datei des Klons.

   + im folgenden Beispiel wird die Parametersyntax angezeigt, die Sie in der Klonspezifikation verwenden:

```
<parameters>
     <parameter>
          <name>log_archive_dest_1</name>
          <value>LOCATION=\mnt\path\clonename\archive</value>
     </parameter>
</parameters>
```

+ + Sie können einen Standardwert verwenden, indem Sie ein Standardelement innerhalb des Parameterelements verwenden. Im folgenden Beispiel übernimmt der Parameter os_Authentication_PREFIX den Standardwert, da das Standardelement angegeben wird:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <default></default>
     </parameter>
</parameters>
```

+ + Sie können einen leeren String als Wert für einen Parameter mithilfe eines leeren Elements angeben. Im folgenden Beispiel wird das os_Authentication_PREFIX auf einen leeren String gesetzt:

+

+

+

```
<parameters>
     <parameter>
          <name>os_authent_prefix</name>
          <value></value>
     </parameter>
</parameters>
```

+ + HINWEIS: Sie können den Wert aus der init.ora-Datei der Quelldatenbank für den Parameter verwenden, indem Sie kein Element angeben.

+ + Wenn ein Parameter mehrere Werte hat, können Sie die durch Kommas getrennten Parameterwerte angeben. Wenn Sie beispielsweise die Datendateien von einem Ort in einen anderen verschieben möchten, können Sie den Parameter db_file_Name_convert verwenden und die durch Kommas getrennten Datendateipfade angeben, wie im folgenden Beispiel zu sehen ist:

+

+

+

```
<parameters>
     <parameter>
          <name>db_file_name_convert</name>
          <value>>\mnt\path\clonename\data file1,\mnt\path\clonename\data
file2</value>
     </parameter>
</parameters>
```

+ + Wenn Sie die Protokolldateien von einem Ort in einen anderen verschieben möchten, können Sie den Parameter log_file_Name_convert verwenden und die durch Kommas getrennten Protokolldateipfade angeben, wie im folgenden Beispiel zu sehen ist:

+

+

+

```
<parameters>
     <parameter>
          <name>log_file_name_convert</name>

<value>>\mnt\path\clonename\archivle1,\mnt\path\clonename\archivle2</value
>
     </parameter>
</parameters>
```

1. Optional: Geben Sie beliebige SQL-Anweisungen an, die für den Klon ausgeführt werden sollen, wenn er online ist.

   Sie können die SQL-Anweisungen verwenden, um Aufgaben auszuführen, wie z. B. das Neuerstellen der temporären Dateien in der geklonten Datenbank.

   Sie müssen sicherstellen, dass am Ende der SQL-Anweisung kein Semikolon enthalten ist.

   Im Folgenden finden Sie eine Beispiel-SQL-Anweisung, die Sie im Rahmen des Klonvorgangs ausführen:

```
<sql-statements>
   <sql-statement>
     ALTER TABLESPACE TEMP ADD
     TEMPFILE 'E:\path\clonename\temp_user01.dbf'
     SIZE 41943040 REUSE AUTOEXTEND ON NEXT 655360
     MAXSIZE 32767M
   </sql-statement>
</sql-statements>
```

Beispiel für Klonspezifikation

Im folgenden Beispiel wird die Klonspezifikationsstruktur für eine Windows-Umgebung angezeigt, einschließlich der Komponenten für die Storage- und Datenbankspezifikation:

```
<clone-specification xmlns="http://www.example.com>

<storage-specification>
    <storage-mapping>
        <mountpoint>
            <source>D:\oracle\<SOURCE SID>_sapdata</source>
            <destination>D:\oracle\<TARGET SID>_sapdata</destination>
        </mountpoint>
    </storage-mapping>
</storage-specification>

<database-specification>
    <controlfiles>
        <file>D:\oracle\<TARGET SID>\origlogA\cntrl\cntrl<TARGET
SID>.dbf</file>
        <file>D:\oracle\<TARGET SID>\origlogB\cntrl\cntrl<TARGET
SID>.dbf</file>
        <file>D:\oracle\<TARGET SID>\sapdata1\cntrl\cntrl<TARGET
SID>.dbf</file>
     </controlfiles>

     <redologs>
        <redogroup>
            <file>D:\oracle\<TARGET SID>\origlogA\log_g11m1.dbf</file>
            <file>D:\oracle\<TARGET SID>\mirrlogA\log_g11m2.dbf</file>
            <number>1</number>
            <size unit="M">100</size>
        </redogroup>
        <redogroup>
            <file>D:\oracle\<TARGET SID>\origlogB\log_g12m1.dbf</file>
            <file>D:\oracle\<TARGET SID>\mirrlogB\log_g12m2.dbf</file>
```

```
            <number>2</number>
            <size unit="M">100</size>
        </redogroup>
        <redogroup>
            <file>D:\oracle\<TARGET SID>\origlogA\log_g13m1.dbf</file>
            <file>D:\oracle\<TARGET SID>\mirrlogA\log_g13m2.dbf</file>
            <number>3</number>
            <size unit="M">100</size>
        </redogroup>
        <redogroup>
            <file>D:\oracle\<TARGET SID>\origlogB\log_g14m1.dbf</file>
            <file>D:\oracle\<TARGET SID>\mirrlogB\log_g14m2.dbf</file>
            <number>4</number>
            <size unit="M">100</size>
       </redogroup>
    </redologs>

    <parameters>
        <parameter>
            <name>log_archive_dest</name>
            <value>LOCATION=>D:\oracle\<TARGET SID>\oraarch</value>
        </parameter>
        <parameter>
            <name>background_dump_dest</name>
            <value>D:\oracle\<TARGET SID>\saptrace\background</value>
        </parameter>
        <parameter>
            <name>core_dump_dest</name>
            <value>D:\oracle\<TARGET SID>\saptrace\background</value>
        </parameter>
        <parameter>
            <name>user_dump_dest</name>
            <value>D:\oracle\<TARGET SID>\saptrace\usertrace</value>
        </parameter>
    </parameters>
   </database-specification>
</clone-specification>
```

Verwandte Informationen

Klonen von Datenbanken und mit benutzerdefinierten Plug-in-Skripten

Klonen von Datenbanken aus Backups

Das Klonen von Datenbanken im aktuellen Status

Überlegungen beim Klonen einer Datenbank auf einem alternativen Host

Klonen von Datenbanken und mit benutzerdefinierten Plug-in-Skripten

SnapManager bietet eine Methode zum Verwenden der benutzerdefinierten Skripte vor und nach einem Klonvorgang. Beispielsweise haben Sie vielleicht ein benutzerdefiniertes Skript erstellt, das eine Klon-Datenbank-SID validiert und sicherstellt, dass die SID von Ihrer Benennungsrichtlinie zulässig ist. Mit dem SnapManager Klon-Plug-in können Sie Ihre benutzerdefinierten Skripts einschließen und sie automatisch vor oder nach einem SnapManager Klonvorgang ausführen lassen.

1. Zeigen Sie Beispielskripts für das Plug-in an.
2. Erstellen Sie ein Skript von Grund auf, oder ändern Sie eines der Beispielskripts für das Plug-in.

   Erstellen Sie Ihr benutzerdefiniertes Skript gemäß den Richtlinien des SnapManager Plug-in-Skripts.
3. Legen Sie Ihr benutzerdefiniertes Skript an einen bestimmten Speicherort für das Verzeichnis.
4. Aktualisieren Sie die XML-Datei für die Klonspezifikation und fügen Sie Informationen zu Ihrem benutzerdefinierten Skript ein, das während des Klonens verwendet werden soll.
5. Überprüfen Sie mit einem SnapManager-Befehl, ob die benutzerdefinierten Skripts betriebsbereit sind.
6. Geben Sie beim Starten des Klonvorgangs den Namen des Skripts und optionale Parameter an.

Klonen von Datenbanken aus Backups

Sie können eine Datenbank aus einer Sicherung klonen, indem Sie den Befehl „Clone create“ verwenden.

Sie müssen zuerst eine Klon-Spezifikations-Datei für die Datenbank erstellen. SnapManager erstellt den Klon auf der Grundlage der Informationen in dieser Spezifikationsdatei.

Sie müssen dem Klon eine neue Oracle System Identifier (SID) geben. Sie können nicht zwei Datenbanken mit derselben SID gleichzeitig auf dem gleichen Host ausführen. Sie können einen Klon auf einem anderen Host haben, der dieselbe SID verwendet. Um einen eindeutigen Namen für den Klon festzulegen, verwenden Sie -Label. Falls Sie diese Option nicht verwenden, erstellt SnapManager einen eindeutigen Namen für den Klon, der SID, Datum und Uhrzeit enthält.

Nachdem Sie eine Datenbank geklont haben, sollten Sie Ihre nsnames.ora-Dateien auf Ihren Clientcomputern mit den neuen geklonten Datenbankverbindungsinformationen aktualisieren. Die tnsnames.ora-Dateien werden verwendet, um eine Verbindung zu einer Oracle-Instanz herzustellen, ohne die vollständigen Datenbankinformationen angeben zu müssen. SnapManager aktualisiert die Dateien nsnames.ora nicht.

SnapManager erstellt immer eine Sicherung einschließlich Archivprotokolldateien, wenn Sie das mit -include -with-Online-Backups erstellte Profil verwenden. SnapManager ermöglicht Ihnen das Klonen nur der vollständigen Datenbank-Backups.

SnapManager (3.2 oder höher) ermöglicht Ihnen, die Backups zu klonen, die die Datendateien und archivierte Log-Dateien enthalten.

Wenn das Archivprotokoll von einem externen Standort aus verfügbar ist, können Sie beim Klonen den externen Standort angeben, um die geklonte Datenbank in einen konsistenten Status wiederherzustellen. Sie müssen sicherstellen, dass Oracle auf den externen Speicherort zugreifen kann. Das Klonen der rein archivprotokollbasierten Backups wird nicht unterstützt.

Obwohl das Backup des Archivprotokolls zusammen mit dem Online-Backup eines partiellen Backups erstellt wird, können Sie mit diesem Backup keinen Datenbankklon erstellen.

Wenn Sie die externen Archivprotokolle angeben, um die geklonte Datenbank in einen konsistenten Status wiederherzustellen, müssen Sie sicherstellen, dass Sie die externen Standortnamen vollständig in Großbuchstaben eingeben. Im Dateisystem müssen sich die Namen aller Ordner und Unterordner in Großbuchstaben befinden, da die Oracle-Datenbank den Zielpfad in Großbuchstaben übersetzt und erwartet, dass sich die externen Zielpfade, Ordnernamen und Unterordnernamen in Großbuchstaben befinden. Wenn Sie die Zielpfade des externen Archivprotokolls in Kleinbuchstaben angeben, kann die Datenbank möglicherweise den angegebenen Pfad nicht identifizieren und kann die geklonte Datenbank nicht wiederherstellen.

Sie können die Datenbanksicherung vom Speicherort der externen Archivprotokolldatei nur für eine eigenständige Datenbank klonen.

Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach dem erfolgreichen oder fehlgeschlagenen Klonvorgang zu sammeln.

Datendatei-Backup ohne Archiv-Log-Backup klonen

Wenn die Datensicherung der Datendateien nicht das Backup des Archivprotokolls umfasst, klont SnapManager für Oracle die Datenbank auf Basis der während des Backups aufgezeichneten Systemänderungsnummer (SCN). Wenn die geklonte Datenbank nicht wiederhergestellt werden kann, wird die für die Fertigstellung der Wiederherstellung erforderliche archivierte Protokolldatei für Thread <number> und Change <SCN> angezeigt, obwohl SnapManager für Oracle die Datenbank weiterhin klont und den Klon schließlich erfolgreich erstellt.

Beim Klonen unter Verwendung der Datendateien Backup ohne Einbindung des Archivprotokolls stellt SnapManager die geklonte Datenbank bis zum letzten Archivprotokoll-SCN wieder her, das während des Backups aufgezeichnet wird.

1. Erstellen einer Clone Specification File.
2. Um einen Klon zu erstellen, geben Sie den folgenden Befehl ein: smo Clone create -Backup -labelBackup_Name-newsidneft_sid-labelclone_Label-profilprofile_Name -clonespepfull_path_to_clonespepfile [-taskspectaskundspecspecSpec] [-recover-from-location] path1 [,<path2>…][-dump]

Verwandte Informationen

Das Klonen von Datenbanken im aktuellen Status

Überlegungen beim Klonen einer Datenbank auf einem alternativen Host

Erstellen von Klonspezifikationen

Der Befehl Smo Clone create

Erstellen von vor-, Post-Task- und Richtlinienskripten

In den Aufgabenskripten verfügbare Variablen für den Klonvorgang

Aufgabenskripte werden erstellt

Speichern der Taskskripte

Das Klonen von Datenbanken im aktuellen Status

Sie können mit einem einzigen Befehl ein Backup und einen Klon der Datenbank aus dem aktuellen Status der Datenbank erstellen.

Wenn Sie das Profil mit der Option -current angeben, erstellt SnapManager zuerst ein Backup und dann einen Klon im aktuellen Status der Datenbank.

Wenn Sie in der Profileinstellung das Backup von Datendateien und Archivprotokollen zum Klonen zusammen aktiviert haben, werden bei jedem Backup der Online-Datendateien auch die Archivprotokolle gesichert. Während des Klonens der Datenbank erstellt SnapManager das Backup der Datendateien zusammen mit dem Archivprotokoll-Backup und erstellt den Datenbankklon. Wenn die Backup des Archivprotokolls nicht enthalten ist, erstellt SnapManager nicht das Backup des Archivprotokolls und kann daher nicht den Klon der Datenbank erstellen.

1. Um die Datenbank im aktuellen Status zu klonen, geben Sie den folgenden Befehl ein: smo Clone create -profileprofile_Name-current -labelclone_name-clonespecclonespec.xml

   Dieser Befehl erstellt sofort ein vollständiges automatisches Backup (das Backup-Label generiert) und erstellt anhand einer vorhandenen Klonspezifikation einen Klon aus diesem Backup.

   Sie können die Option -dump als optionalen Parameter angeben, um die Dump-Dateien nach den erfolgreichen oder fehlgeschlagenen Vorgängen zu sammeln. Der Dump wird sowohl für die Backup- als auch für Klonvorgänge erfasst.

Klonen von Datenbank-Backups ohne Umsetzungsprotokolle

SnapManager ermöglicht Ihnen ein flexibles Klonen, sodass Sie die geklonte Datenbank manuell bis zu einem gewünschten Zeitpunkt wiederherstellen können, ohne die Datenbank über ResetLogs zu öffnen. Sie können die geklonte Datenbank auch manuell als Data Guard Standby-Datenbank konfigurieren.

Wenn Sie die Option -no-resetlogs beim Erstellen des Klons auswählen können, führt SnapManager die folgenden Aktivitäten aus, um die geklonte Datenbank zu erstellen:

1. Führt die Vorverarbeitung, falls angegeben, vor dem Start des Klonvorgangs aus
2. Erstellt die geklonte Datenbank mit der vom Benutzer angegebenen SID
3. Führt die SQL-Anweisungen aus, die für die geklonte Datenbank ausgegeben wurden.

   Nur die SQL-Anweisungen, die im Mount-Status ausgeführt werden können, wurden erfolgreich ausgeführt.

4. Führt die Aktivität der Aufgabe nach der Verarbeitung aus, falls angegeben.

Welche Aufgaben müssen Sie tun, um die geklonte Datenbank manuell wiederherzustellen

1. Mounten Sie die Archiv-Log-Backups und stellen Sie die geklonte Datenbank manuell wieder her, indem Sie die Archiv-Log-Dateien vom gemounteten Pfad verwenden.
2. Öffnen Sie nach der Durchführung manueller Wiederherstellung die wiederhergestellte geklonte Datenbank mit der Option -Resetlogs.

3. Erstellen Sie bei Bedarf temporäre Tablespaces.
4. Führen Sie das DBNEWID-Dienstprogramm aus.
5. Gewähren sie den Anmeldeinformationen der geklonten Datenbank sysdba-Berechtigung.

Beim Klonen der Datenbank-Backups mit der Option -no-resetlogs lässt SnapManager die geklonte Datenbank im gemounteten Status zur manuellen Wiederherstellung zurück.

Die mit der Option -no-resetlogs erstellte geklonte Datenbank ist keine vollständige Datenbank. Daher dürfen Sie SnapManager Operationen auf dieser Datenbank nicht ausführen, obwohl SnapManager Sie nicht daran hindert, irgendwelche Operationen auszuführen.

Wenn Sie die Option -no-resetlogs nicht angeben, wendet SnapManager die Archiv-Log-Dateien an und öffnet die Datenbank mit Resetlogs.

1. Geben Sie den folgenden Befehl ein: smo Clone create -profilprofile_Name [-Backup-labelbackup_Name in den folgenden Fällen: -Backup-idBackup_id current] -newsidneft_sid-clonespepfull_path_to_clonespepfile -no-resetlogs

   Wenn Sie versuchen, sowohl -no-resetlogs als auch Recovery-from-location Optionen anzugeben, erlaubt SnapManager nicht, diese beiden Optionen zusammen anzugeben, und zeigt die Fehlermeldung an: SMO-04084: Sie müssen entweder eine der Optionen angeben: -No-resetlogs oder -Recovery-from-location.

Beispiel

```
smo clone create -profile product -backup-label full_offline -newsid
PROD_CLONE -clonespec prod_clonespec.xml -label prod_clone-reserve -no
-reset-logs
```

Überlegungen beim Klonen einer Datenbank auf einem alternativen Host

Bevor Sie auf einem anderen Host als dem Klon der Datenbank klonen können, müssen einige Anforderungen erfüllt werden.

Folgende Tabelle zeigt die Setup-Anforderungen für Quell- und Zielhost:

Vorbedingung eingerichtet	Anforderungen
Der Netapp Architektur Sind	Muss auf den Quell- und Ziel-Hosts identisch sein
Betriebssystem und Version	Muss auf den Quell- und Ziel-Hosts identisch sein
SnapManager für Oracle	Muss auf den Quell- und Ziel-Hosts installiert und ausgeführt werden
Anmeldedaten	Muss festgelegt werden, damit der Benutzer auf den Zielhost zugreifen kann

Oracle	Die Software-Version muss auf den Quell- und Ziel-Hosts installiert sein. Der Oracle-Listener muss auf dem Ziel-Host ausgeführt werden.
Kompatibler Storage Stack	Muss auf den Quell- und Ziel-Hosts identisch sein
Protokoll für den Zugriff auf Datendateien	Muss auf den Quell- und Ziel-Hosts identisch sein
Domäne	Sowohl der Remote-Host als auch der Host, auf dem sich die Datenbank befindet, müssen sich in der Domäne und nicht in der Arbeitsgruppe befinden

Klonen einer Datenbank auf einem alternativen Host

Sie können mit dem Befehl Clone create ein Datenbank-Backup auf einem alternativen Host klonen.

- Erstellen Sie ein Profil oder haben Sie ein vorhandenes Profil.
- Erstellen Sie ein vollständiges Backup oder ein bereits vorhandenes Datenbank-Backup.
- Erstellen Sie eine Klonspezifikation oder weisen Sie eine vorhandene Klonspezifikation auf.
  a. Geben Sie zum Klonen einer Datenbank auf einem anderen Host den folgenden Befehl ein: smo Clone create -Backup-Label Backup_Label_Name-newsid New_sid-Host Target_Host-Label Clone_Label-commentcomment_Text-profileprofile_Name-clonepec full_path_to_clonespefile

     Oracle lässt Sie nicht zwei Datenbanken mit derselben SID gleichzeitig auf dem gleichen Host laufen. Aus diesem Grund müssen Sie für jeden Klon eine neue SID angeben. Sie können jedoch eine Datenbank auf einem anderen Host mit derselben SID haben.

Verwandte Informationen

Profile werden erstellt

Klonen von Datenbanken aus Backups

Erstellen von Klonspezifikationen

Der Befehl Smo Clone create

Anzeigen einer Liste von Klonen

Sie können eine Liste von Klonen anzeigen, die mit einem bestimmten Profil verknüpft sind.

Die Liste enthält die folgenden Informationen über die Klone in einem Profil:

- Die ID für den Klon
- Der Status des Klonvorgangs

- Oracle SID für den Klon
- Host, auf dem sich der Klon befindet
- Etikett für den Klon

Wenn Sie die Option -verbose angeben, werden in der Ausgabe auch die Kommentare für den Klon angezeigt.

1. Um eine Liste aller Klone für ein Profil anzuzeigen, geben Sie den folgenden Befehl ein: Smo Clone list -profile Profile_Name [-quiet / -verbose]

Verwandte Informationen

Der Befehl smo Clone list

Anzeigen detaillierter Kloninformationen

Mit dem Befehl Clone show können Sie ausführliche Informationen über einen bestimmten Klon anzeigen.

Mit dem Befehl Clone show werden die folgenden Informationen angezeigt:

- Systemidentifikation und Klon-ID klonen
- Status des Klonvorgangs
- Start- und Enddatum bzw. -Uhrzeit des Klons
- Klonbezeichnung
- Klonkommentar
- Backup-Label und -ID
- Quelldatenbank
- Start- und Endzeit des Backups
- Datenbankname, Tabellen und Datendateien
- Host-Name und Dateisysteme mit Datendateien
- Storage-System-Volumes und Snapshot-Kopien, die den Klon sichern
    a. Geben Sie den folgenden Befehl ein: smo Clone show -profile profile_Name [-Label Label [-id guid]

Verwandte Informationen

Der Befehl smo Clone show

Klone werden gelöscht

Sie können die Klone löschen, wenn die Größe der Snapshot-Kopie zwischen 10 % und 20 % des Backups reicht. Dies garantiert außerdem, dass der Klon die aktuellsten Daten enthält.

Die Bezeichnung ist die eindeutige Kennung für jeden Klon in einem Profil. Sie können den Klon mit dem Klonnamen oder der ID, jedoch nicht mit der System-ID (SID) löschen.

Die Klon-SID und die Klonbezeichnung sind nicht identisch.

Wenn Sie einen Klon löschen, muss die Datenbank ausgeführt werden. Andernfalls werden viele Dateien und Verzeichnisse für den vorhandenen Klon nicht gelöscht. Dies führt zu mehr Arbeit, bevor ein weiterer Klon erstellt werden kann.

Die für bestimmte Oracle-Parameter im Klon angegebenen Verzeichnisse werden beim Löschen des Klons zerstört und sollten nur Daten für die geklonte Datenbank enthalten: Archivprotokoll-Ziele, Hintergrund-, Core- und BenutzerabDump-Ziele. Die Audit-Dateien werden nicht gelöscht.

Sie können einen Klon nicht löschen, wenn der Klon in anderen Vorgängen verwendet wird.

Optional können Sie die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen Klonlöschen sammeln.

1. Geben Sie den folgenden Befehl ein: smo Clone delete -profile Profile_Name [-Label_ID guid][-Force][-dump][-quiet][-verbose]

Beispiel

```
smo clone delete -profile targetdb1_prof1 -label sales0908_clone1
```

Verwandte Informationen

Der Befehl smo Clone delete

Einführung in Datensicherung in SnapManager

SnapManager unterstützt Datensicherung zum Schutz der Backups auf sekundären oder tertiären Storage-Systemen. Sie müssen SnapMirror und SnapVault Beziehungen zwischen den Quell- und Ziel-Volumes einrichten.

Mit den Post-Backup-Skripts können die Backups sowohl von der Befehlszeilenschnittstelle (CLI) als auch von der grafischen Benutzeroberfläche (GUI) auf einem Primärspeichersystem geschützt werden.

Wie SnapManager Backups auf dem lokalen Storage aufbewahrt

Mit SnapManager können Sie Backups erstellen, die Aufbewahrungsrichtlinien erfüllen, die angeben, wie viele erfolgreiche Backups auf lokalem Storage aufbewahrt werden sollen. Sie können die Anzahl erfolgreicher Backups angeben, die im Profil für eine bestimmte Datenbank aufbewahrt werden sollen.

Sie können Backups für folgende erstellen:

- 10 Tage tägliche Backups auf dem Primärspeicher
- 2 Monate monatliche Backups auf dem Primärspeicher
- 7 Tage tägliche Backups auf dem Sekundärspeicher
- 4 Wochen wöchentliche Backups auf dem Sekundärspeicher
- 6 Monate monatliche Backups auf dem Sekundärspeicher

Sie können für jedes Profil in SnapManager die Werte für die folgenden nicht begrenzten Aufbewahrungsklassen ändern:

- Stündlich
- Täglich
- Wöchentlich
- Monatlich

SnapManager legt fest, ob ein Backup aufbewahrt werden soll, indem sowohl die Anzahl der Aufbewahrung (z. B. 15 Backups) als auch die Aufbewahrungsdauer (z. B. 10 Tage tägliche Backups) berücksichtigt werden. Ein Backup läuft ab, wenn sein Alter die für seine Aufbewahrungsklasse festgelegte Aufbewahrungsdauer überschreitet oder die Anzahl der Backups die Aufbewahrungsdauer überschreitet. Beispiel: Wenn die Backup-Anzahl 15 beträgt (SnapManager hat 15 erfolgreiche Backups erstellt) und die Dauer für tägliche Backups von 10 Tagen festgelegt wird, laufen die fünf ältesten erfolgreichen geeigneten Backups ab.

Nach Ablauf eines Backups wird das abgelaufene Backup entweder von SnapManager entfernt oder gelöscht. SnapManager behält immer das letzte Backup bei.

SnapManager zählt nur die Anzahl erfolgreicher Backups für die Aufbewahrungszahl. Es werden folgende Punkte nicht berücksichtigt:

Backups, die nicht in der Aufbewahrungsanzahl enthalten sind	Zusätzliche Angaben
Fehlgeschlagene Backups	SnapManager behält die Informationen zu erfolgreichen und fehlgeschlagenen Backups bei. Obwohl fehlgeschlagene Backups nur einen minimalen Speicherplatz im Repository benötigen, können Sie diese auch löschen. Fehlgeschlagene Backups verbleiben im Repository, bis Sie sie löschen.
Backups, die für die Aufbewahrung vorgesehen sind, unbegrenzt oder für eine andere Aufbewahrungsklasse Backups	SnapManager löscht keine Backups, die für die Aufbewahrung vorgesehen sind. Darüber hinaus berücksichtigt SnapManager nur die Backups in derselben Aufbewahrungsklasse (beispielsweise berücksichtigt SnapManager nur die stündlichen Backups für die stündliche Aufbewahrungszahl).
Backups werden über lokalen Storage gemountet	Wenn Snapshot Kopien angehängt werden, sind sie auch geklont und gelten somit nicht als für die Aufbewahrung geeignet. SnapManager kann die Snapshot Kopien nicht löschen, wenn sie geklont sind.
Backups, die zum Erstellen eines Klons im lokalen Storage verwendet werden	SnapManager behält alle Backups, die zum Erstellen von Klonen verwendet werden, berücksichtigt diese jedoch nicht für die Anzahl der Backup-Aufbewahrung.

SnapManager bietet für jede Aufbewahrungsklasse eine Standardanzahl und -Dauer. Beispielsweise behalten

SnapManager für die Anzahl der stündlichen Aufbewahrungsklassen standardmäßig vier Backups pro Stunde bei. Sie können diese Standardwerte überschreiben und beim Erstellen oder Aktualisieren des Profils die Werte festlegen oder die Standardwerte für die Anzahl und Dauer der Aufbewahrung in der Datei smo.config ändern.

Wenn lokale Backups aufgrund der Aufbewahrungsrichtlinie ablaufen, werden die Backups gelöscht.

Bei einem nur-archivlog Backup Vorgang archiviert SnapManager die Redo-Log-Dateien nicht, anders als beim Online-Datenbank-Backup-Prozess. Sie müssen ein Pre-Task-Skript hinzufügen, um die Redo-Log-Dateien zu archivieren, bevor Sie den nur-Archivprotokoll durchführen. Das Vortaskskript muss den Befehl Logfile ändern System Switch ausführen.

Das folgende Beispiel zeigt die Maßnahmen, die SnapManager für verschiedene Arten von Backups ergreift, basierend auf einer Aufbewahrungsrichtlinie für drei tägliche Backups (wobei die Anzahl auf Aufbewahrung 3 festgelegt ist):

Backup-Datum	Status	Maßnahmen zur Aufbewahrungsrichtlinie ergriffen	Erklärung
5/10	Erfolgreich	Bitte Halten	Es handelt sich um das aktuellste erfolgreiche Backup und wird daher beibehalten.
5/9	Erfolgreich, geklont	Überspringen	SnapManager berücksichtigt keine Backups, die zum Klonen in der Anzahl der Aufbewahrungsrichtlinien verwendet werden. Dieses Backup entfällt auf die Anzahl erfolgreicher Backups.
5/8	Erfolgreich, angehängt	Überspringen	SnapManager berücksichtigt keine gemounteten Backups in der Anzahl der Aufbewahrungsrichtlinien. Dieses Backup entfällt auf die Anzahl erfolgreicher Backups.
5/7	Fehlgeschlagen	Überspringen	Fehlgeschlagene Backups werden nicht gezählt.
5/5	Erfolgreich	Bitte Halten	SnapManager hält dieses zweite erfolgreiche tägliche Backup.

5/3	Erfolgreich	Bitte Halten	SnapManager hält dieses dritte erfolgreiche tägliche Backup.
5/2	Erfolgreich	Löschen	SnapManager zählt dieses erfolgreiche Backup, aber nachdem SnapManager drei erfolgreiche tägliche Backups erreicht hat, wird dieses Backup gelöscht.

Verwandte Informationen

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Überlegungen zur Durchführung der Datensicherung

Beachten Sie bei der Durchführung von Datensicherung bestimmte Überlegungen.

- Um Klon- oder Wiederherstellungsvorgänge von sekundären Systemen durchzuführen, müssen Sie das Ziel-Volume im Namespace mounten und ordnungsgemäß exportieren.
- Sie müssen den SnapDrive-Konfigurationsparameter „Check-Export-Permission-nfs-Clone“ deaktivieren, indem Sie den Wert auf „aus“ setzen.

  Die Dokumentation zu SnapDrive für UNIX auf der NetApp Support-Website enthält zusätzliche Informationen zum Parameter Check-Export-Permission-nfs-Clone.

- Sie müssen die SnapMirror Beziehung für die angeforderten sekundären Storage-Volumes im sekundären Storage-System konfigurieren.
- Sie müssen die SnapVault-Beziehung für die angeforderten sekundären Storage-qtrees im sekundären Storage-System für Data ONTAP 7-Mode konfigurieren.
- Sie müssen eine Richtlinie und Regeln für das benutzerdefinierte SnapMirror-Etikett definieren, wenn Sie SnapVault Post-Script für Clustered Data ONTAP verwenden.

  SnapVault Post-Script unterstützt geclusterte Data ONTAP Volumes und die SnapMirror Beziehungstypen DP und XDP. Die ONTAP-Dokumentation auf der NetApp Support-Website enthält Informationen zur Konfiguration von SnapMirror und SnapVault.

"Dokumentation auf der NetApp Support Site: mysupport.netapp.com"

Lizenzen für Datensicherung in SnapManager erforderlich

Sie müssen sicherstellen, dass die für die Datensicherung erforderlichen Lizenzen auf den primären und sekundären Storage-Systemen installiert und aktiviert werden.

Primäre Speichersysteme erhalten die aktuellsten Transaktions-Updates für die Oracle-Datenbank, speichern die Daten und stellen lokalen Backup-Schutz der Datenbank sicher. Das primäre Storage-System verwaltet außerdem Datenbankdatendateien, Log-Dateien und Kontrolldateien. Sekundäre Speichersysteme fungieren als Remote-Speicher für die geschützten Backups.

Zur Datensicherung müssen auf den primären Storage-Systemen die folgenden Lizenzen installiert und aktiviert sein:

> Wenn Sie die Datensicherung auf den sekundären Storage-Systemen aktivieren möchten, müssen Sie diese Lizenzen auch auf den sekundären Storage-Systemen installieren und aktivieren.

- Data ONTAP 7-Mode (7.3.1 oder höher) oder Clustered Data ONTAP (8.2 oder höher)
- SnapVault
- SnapRestore
- SnapMirror
- Zum Klonen ist FlexClone erforderlich.

  FlexClone ist außerdem nur erforderlich, wenn SnapDrive für die Verwendung von FlexClone in SAN-Umgebungen konfiguriert ist.

- Das entsprechende Protokoll, z. B. iSCSI (Internet Small Computer System Interface) oder Fibre Channel (FC)

Sicherung von Datenbank-Backups mithilfe von Postskripten

SnapManager ermöglicht Ihnen, Datenbank-Backups mithilfe von Postskripten zu schützen, wenn eine SnapMirror oder SnapVault Beziehung zwischen den primären und sekundären Storage-Systemen hergestellt wird. Es können Standard-Postskripte für die Nachbearbeitung des Backup-Vorgangs über die SnapManager CLI und GUI verwendet werden.

Folgende Standard-Postscripts sind unter default_install_Directory\Plugins\Backup\create\post verfügbar:

- Das SnapMirror Postscript, Mirror_the_Backup.cmd wenn sie Data ONTAP in 7-Mode verwenden
- Das SnapVault Postscript Vault_the_Backup.cmd, wenn Sie Data ONTAP in 7-Mode verwenden
- Das SnapMirror Postscript, Mirror_the_Backup_cDOT.cmd wenn sie Clustered Data ONTAP verwenden
- Das SnapVault Postscript Vault_the_Backup_cDOT.cmd wenn sie Clustered Data ONTAP verwenden

Weitere Informationen finden Sie in der Version readme.txt unter default_install_Directory\Plugins.

SnapManager 3.1 oder eine frühere Version bietet Vorverarbeitung- oder Nachbearbeitungsskripten nur für Klonvorgänge. SnapManager 3.2 oder höher bietet Vorverarbeitungs- und Nachbearbeitungsskripte für Backup- und Restore-Vorgänge. Diese Skripte können vor oder nach den Backup- oder Wiederherstellungsvorgängen ausgeführt werden.

> Die Skripte werden nur als Referenz bereitgestellt. Sie wurden mit SnapDrive 7.0 für Windows oder höher oder höher getestet, funktionieren aber möglicherweise nicht in allen Umgebungen. Sie sollten die Skripte auf der Grundlage Ihrer Anforderungen für den sekundären Schutz anpassen. Die Skripte funktionieren nicht mit SnapDrive Versionen vor 6.2.

Beispiel für Nachskripte

Sie können mithilfe von Beispielskripten darauf verweisen und angepasste Skripte

erstellen, um eine Spiegelung und Vaulting durchzuführen. Die Beispielskripte sind unter default_install_Directory\Plugins\Backup\create\post verfügbar.

Mirror_the_Backup.cmd

Wenn Sie Data ONTAP 7-Mode verwenden, können Sie dieses Beispielskript zur Spiegelung des Backups nutzen. Sie umfasst drei Operationen (Prüfen, beschreiben und ausführen) und führt sie am Ende des Skripts aus. Das Skript umfasst auch die Handhabung von Fehlermeldungen mit den Codes 0 bis 4 und > 4:

```
@echo off
REM $Id:
//depot/prod/capstan/main/src/plugins/windows/examples/backup/create/post/
Mirror_the_backup.cmd#1 $
REM
REM Copyright \(c\) 2011 NetApp, Inc.
REM All rights reserved.
REM
REM
REM This is a sample post-task script to mirror the volumes to the
secondary storage after successful backup operation.
REM|-------------------------------------------------------------------------
----------------------------------------|
REM| Pre-requisite/Assumption:
|
REM|   SnapMirror relationship for the requested secondary storage volumes
must be configured in Secondary storage. |
REM|-------------------------------------------------------------------------
----------------------------------------|
REM
REM
REM This script can be used from the SnapManager graphical user interface
(GUI) and command line interface (CLI).
REM
REM To execute the post-task script for the backup operation from
SnapManager GUI, follow these steps:
REM  1. From the Backup wizard > Task Specification page > Post-Tasks tab
> select the post-task scripts from the Available Scripts section.
REM
REM
REM To execute the post-task script for the backup operation from
SnapManager CLI, follow these steps:
REM  1. create a task specification XML file.
REM  2. Add the post-script name in the <post-tasks> tag of the XML file.
REM
REM Example:
REM              <post-tasks>
REM                 <task>
```

```
REM                    <name>Mirror the backup</name>
REM                      <description>Mirror the backup</description>
REM                </task>
REM              <post-tasks>
REM
REM
REM
REM IMPORTANT NOTE: This script is provided for reference only. It has
been tested with SnapDrive 6.3.0 for Windows but may not work in all
environments.  Please review and then customize based on your secondary
protection requirements.
REM
set /a EXIT=0
set name="Mirror the backup"
set description="Mirror the backup"
set parameter=()


if /i "%1" == "-check" goto :check
if /i "%1" == "-execute" goto :execute
if /i "%1" == "-describe" goto :describe

:usage
        echo usage: %0 ^{ -check ^| -describe ^| -execute ^}
        set /a EXIT=99
        goto :exit

:check
        set /a EXIT=0
        goto :exit

:describe
        echo SM_PI_NAME:%name%
        echo SM_PI_DESCRIPTION:%description%
        echo SM_PRIMARY_MOUNT_POINTS : %SM_PRIMARY_MOUNT_POINTS%
        set /a EXIT=0
        goto :exit

REM - Split the comma-separated PRIMARY_MOUNT_POINTS and Mirror the
PRIMARY_MOUNT_POINTS one-by-one.

:execute
        set /a EXIT=0

        echo "execution started"
```

```
        REM FOR %%G IN (%SM_PRIMARY_MOUNT_POINTS%) DO echo %%G

        FOR %%V IN (%SM_PRIMARY_MOUNT_POINTS%) DO sdcli snap update_mirror
-d %%V

        if "%ERRORLEVEL%" NEQ "0" (
           set /a EXIT=4
           exit /b %EXIT%
        )

        echo "execution ended"

        goto :exit

:exit
        echo Command complete.
        exit /b %EXIT%
```

Vault_the_Backup.cmd

Wenn Sie Data ONTAP in 7-Mode verwenden, können Sie dieses Beispielskript für die Sicherung verwenden. Sie umfasst drei Operationen (Prüfen, beschreiben und ausführen) und führt sie am Ende des Skripts aus. Das Skript umfasst auch die Handhabung von Fehlermeldungen mit den Codes 0 bis 4 und > 4:

```
@echo off
REM $Id:
//depot/prod/capstan/main/src/plugins/windows/examples/backup/create/post/
Vault_the_backup.cmd#1 $
REM
REM Copyright \(c\) 2011 NetApp, Inc.
REM All rights reserved.
REM
REM
REM This is a sample post-task script to vault the qtrees to the secondary
storage after successful backup operation.
REM|-------------------------------------------------------------------------
----------------------------------------|
REM| Pre-requisite/Assumption:
|
REM|   SnapVault relationship for the requested secondary storage qtrees
must be configured in Secondary storage. |
REM|-------------------------------------------------------------------------
----------------------------------------|
REM
REM
REM This script can be used from the SnapManager graphical user interface
```

```
(GUI) and command line interface (CLI).
REM
REM To execute the post-task script for the backup operation from
SnapManager GUI, follow these steps:
REM  1. From the Backup wizard > Task Specification page > Post-Tasks tab
> select the post-task scripts from the Available Scripts section.
REM
REM
REM To execute the post-task script for the backup operation from
SnapManager CLI, follow these steps:
REM  1. create a task specification XML file.
REM  2. Add the post-script name in the <post-tasks> tag of the XML file.
REM
REM Example:
REM              <post-tasks>
REM                 <task>
REM                    <name>Vault the backup</name>
REM                    <description>Vault the backup</description>
REM                </task>
REM              <post-tasks>
REM
REM IMPORTANT NOTE: This script is provided for reference only. It has
been tested with SnapDrive 6.3.0 for Windows but may not work in all
environments.  Please review and then customize based on your secondary
protection requirements.
REM
REM
REM
REM
REM
set /a EXIT=0
set name="Vault the backup"
set description="Vault the backup"
set parameter=()



if /i "%1" == "-check" goto :check
if /i "%1" == "-execute" goto :execute
if /i "%1" == "-describe" goto :describe

:usage
        echo usage: %0 ^{ -check ^| -describe ^| -execute ^}
        set /a EXIT=99
        goto :exit
```

```
:check
        set /a EXIT=0
        goto :exit

:describe
        echo SM_PI_NAME:%name%
        echo SM_PI_DESCRIPTION:%description%
        echo SM_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS :
%SM_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS%
        set /a EXIT=0
        goto :exit

REM Split the colon-separated SM_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS And
SnapVault the mountpoints one-by-one

:execute
        set /a EXIT=0

        echo "execution started"

        FOR %%A IN (%SM_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS%) DO FOR /F
"tokens=1,2 delims=:" %%B IN ("%%A") DO sdcli snapvault archive  -a %%B
-DS %%C %%B

        if "%ERRORLEVEL%" NEQ "0" (
           set /a EXIT=4
           exit /b %EXIT%
        )
        echo "execution ended"

        goto :exit

:exit
        echo Command complete.
        exit /b %EXIT%
```

Mirror_the_Backup_cDOT.cmd

Wenn Sie Clustered Data ONTAP verwenden, können Sie dieses Beispielskript zur Spiegelung des Backups nutzen. Sie umfasst drei Operationen (Prüfen, beschreiben und ausführen) und führt sie am Ende des Skripts aus. Das Skript umfasst auch die Handhabung von Fehlermeldungen mit den Codes 0 bis 4 und > 4:

```
@echo off
REM $Id:
//depot/prod/capstan/main/src/plugins/windows/examples/backup/create/post/
Mirror_the_backup_cDOT.cmd#1 $
```

```
REM
REM  Copyright \(c\) 2011 NetApp, Inc.
REM All rights reserved.
REM
REM
REM This is a sample post-task script to mirror the volumes to the
secondary storage after successful backup operation.
REM|-------------------------------------------------------------------
----------------------------------------|
REM| Pre-requisite/Assumption:
|
REM|   SnapMirror relationship should be set for the primary volumes and
secondary volumes                          |
REM|-------------------------------------------------------------------
----------------------------------------|
REM
REM
REM This script can be used from the SnapManager graphical user interface
(GUI) and command line interface (CLI).
REM
REM To execute the post-task script for the backup operation from
SnapManager GUI, follow these steps:
REM  1. From the Backup wizard > Task Specification page > Post-Tasks tab
> select the post-task scripts from the Available Scripts section.
REM
REM
REM To execute the post-task script for the backup operation from
SnapManager CLI, follow these steps:
REM  1. create a task specification XML file.
REM  2. Add the post-script name in the <post-tasks> tag of the XML file.
REM
REM Example:
REM             <preposttask-specification xmlns="http://www.netapp.com">
REM               <task-specification>
REM                 <post-tasks>
REM                   <task>
REM                     <name>"Mirror the backup for cDOT"</name>
REM                   </task>
REM                 </post-tasks>
REM               </task-specification>
REM             </preposttask-specification>
REM
REM
REM
REM IMPORTANT NOTE: This script is provided for reference only. It has
been tested with SnapDrive 7.0 for Windows but may not work in all
```

```
environments.  Please review and then customize based on your secondary
protection requirements.
REM
set /a EXIT=0
set name="Mirror the backup cDOT"
set description="Mirror the backup cDOT"
set parameter=()



if /i "%1" == "-check" goto :check
if /i "%1" == "-execute" goto :execute
if /i "%1" == "-describe" goto :describe

:usage
        echo usage: %0 ^{ -check ^| -describe ^| -execute ^}
        set /a EXIT=99
        goto :exit

:check
        set /a EXIT=0
        goto :exit

:describe
        echo SM_PI_NAME:%name%
        echo SM_PI_DESCRIPTION:%description%
        set /a EXIT=0
        goto :exit

REM - Split the comma-separated SM_PRIMARY_MOUNT_POINTS then Mirror the
PRIMARY_MOUNT_POINTS one-by-one.

:execute
        set /a EXIT=0

        echo "execution started"

        REM FOR %%G IN (%SM_PRIMARY_MOUNT_POINTS%) DO powershell.exe -file
"c:\snapmirror.ps1" %%G < CON

        powershell.exe -file "c:\snapmirror.ps1"
%SM_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG% < CON


        if "%ERRORLEVEL%" NEQ "0" (
           set /a EXIT=4
           exit /b %EXIT%
```

```
        )

        echo "execution ended"

        goto :exit

:exit
        echo Command complete.
        exit /b %EXIT%
```

Vault_the_Backup_cDOT.cmd

Wenn Sie Clustered Data ONTAP verwenden, können Sie dieses Beispielskript als Vault des Backups verwenden. Sie umfasst drei Operationen (Prüfen, beschreiben und ausführen) und führt sie am Ende des Skripts aus. Das Skript umfasst auch die Handhabung von Fehlermeldungen mit den Codes 0 bis 4 und > 4:

```
@echo off
REM $Id:
//depot/prod/capstan/main/src/plugins/windows/examples/backup/create/post/
Vault_the_backup_cDOT.cmd#1 $
REM
REM  Copyright \(c\) 2011 NetApp, Inc.
REM All rights reserved.
REM
REM
REM This is a sample post-task script to do vault update to the secondary
storage after successful backup operation.
REM|-------------------------------------------------------------------------
-----------------------------------------|
REM| Pre-requsite/Assumption:
|
REM|   Vaulting relationship with policy and rule needs to be established
between primary and secondary storage volumes |
REM|-------------------------------------------------------------------------
-----------------------------------------|
REM
REM
REM This script can be used from the SnapManager graphical user interface
(GUI) and command line interface (CLI).
REM
REM To execute the post-task script for the backup operation from
SnapManager GUI, follow these steps:
REM
REM  1. From the Backup wizard > Task Specification page > Post-Tasks tab
> select the post-task scripts from the Available Scripts section.
REM  2. You can view the parameters available in the post-task script in
```

```
the Parameter section of the Task Specification page.
REM  3. Provide values to the following parameters:
REM     SNAPSHOT_LABEL     - Label Name to be set for snapshots before
doing the vault update
REM
REM FOR WINDOWS ITS ADVISED TO USE THE post-task script FROM THE GUI BY
SAVING THE BELOW SPEC XML AND GIVING THIS IN THE GUI LOAD XML FILE .
REM
REM To execute the post-task script for the backup operation from
SnapManager CLI, follow these steps:
REM  1. create a task specification XML file.
REM  2. Add the post-script name in the <post-tasks> tag of the XML file .
REM Example:
REM             <preposttask-specification xmlns="http://www.netapp.com">
REM               <task-specification>
REM                 <post-tasks>
REM                   <task>
REM                     <name>"Vault the backup for cDOT"</name>
REM                     <parameter>
REM                     <name>SNAPSHOT_LABEL</name>
REM                     <value>TST</value>
REM                     </parameter>
REM                   </task>
REM                 </post-tasks>
REM               </task-specification>
REM             </preposttask-specification>
REM
REM
REM IMPORTANT NOTE: This script is provided for reference only. It has
been tested with SnapDrive 7.0.0 for Windows but may not work in all
environments.
Please review and then customize based on your secondary protection
requirements.
REM
REM
REM Need to take care of the parameter variable, its not like shell script
array handling, so declare a new variable
REM for one more argument and set that variable SM_PI_PARAMETER in the
describe method. Then only that variable will be
REM Visible in the GUI task specification wizard else it wont list.

set /a EXIT=0
set name="Vault the backup for cDOT"
set description="Vault the backup For cDOT volumes"
set parameter=SNAPSHOT_LABEL :
```

```
if /i "%1" == "-check" goto :check
if /i "%1" == "-execute" goto :execute
if /i "%1" == "-describe" goto :describe

:usage
        echo usage: %0 ^{ -check ^| -describe ^| -execute ^}
        set /a EXIT=99
        goto :exit

:check
        set /a EXIT=0
        goto :exit

:describe
        echo SM_PI_NAME:%name%
        echo SM_PI_DESCRIPTION:%description%
    echo SM_PI_PARAMETER:%parameter%

        set /a EXIT=0
        goto :exit

REM Split the colon-separated SM_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS And
SnapVault the mountpoints one-by-one

:execute
        set /a EXIT=0

    echo "execution started"

    powershell.exe -file "c:\snapvault.ps1"
%SM_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG%  %SNAPSHOT_LABEL% < CON

        if "%ERRORLEVEL%" NEQ "0" (
           set /a EXIT=4
           exit /b %EXIT%
        )
    echo "execution ended"

        goto :exit

:exit
        echo Command complete.
        exit /b %EXIT%
```

Erstellen oder Aktualisieren der Postskripte

Sie können entweder neue Post-Skripte erstellen oder die Skripte verwenden, die unter default_install_Directory\Plugins\Backup\create\post verfügbar sind.

Das Skript muss so strukturiert werden, dass es im Kontext einer SnapManager Operation ausgeführt werden kann. Erstellen Sie das Skript auf der Grundlage der erwarteten Vorgänge, der verfügbaren Eingabeparameter und der Rückgabekonventionen.

1. Erstellen Sie ein neues Skript oder verwenden Sie die verfügbaren Beispielskripte.
2. Ändern oder schließen Sie die Funktionen, Variablen und Parameter nach Bedarf an.
3. Speichern Sie das benutzerdefinierte Skript.
4. Fügen Sie den Skriptnamen und die erforderlichen Eingaben in der XML-Datei für die Aufgabe nach der Verarbeitung hinzu oder geben Sie die Eingaben aus der GUI durch Auswahl des richtigen Skripts und Eingabeparameters an.

> Sie müssen keine sekundären Speicherdetails in der XML-Datei für die Aufgabenspezifikation angeben.

Verwandte Informationen

Erstellen von Aufgabenspezifikationsdatei und Skripten für SnapManager-Vorgänge

Erstellen von Dateien für die Nachverarbeitung und Aufgabenspezifikation

Mit SnapManager können Sie XML-Dateien nach der Verarbeitung mit Aufgabenspezifikation für den Backup-Vorgang erstellen, einschließlich der Post-Skripte SnapMirror oder SnapVault. Die Skripte ermöglichen die Spiegelung oder Vault des Backups auf sekundären Speicher.

1. Öffnen Sie eine neue XML-Datei.

   Die XML-Beispieldatei für die Aufgabenspezifikation kann unter default_install_Directory\Plugins\examples angezeigt werden.

2. Fügen Sie den Skriptnamen als Eingabeparameter hinzu.
3. Speichern Sie die XML-Datei für die Aufgabenspezifikation.

Verwenden der Aufgabenspezifikation für die Nachbearbeitung, um Volumes zu spiegeln

Mit SnapManager für Oracle können Sie das Skript zur Spiegelung der Volumes verwenden, nachdem der Backup-Vorgang in einer Windows Umgebung durchgeführt wurde.

1. Erstellen Sie eine XML-Datei für die Aufgabenspezifikation.
2. Geben Sie in der XML-Datei den Skriptnamen als Eingabeparameter ein.
3. Speichern Sie die XML-Datei für die Aufgabenspezifikation.
4. Erstellen Sie mit dem folgenden Befehl ein geschütztes Backup der Datenbank auf dem sekundären Speicher.

Beim Erstellen des geschützten Backups müssen Sie nach der Option -taskSpec den vollständigen Pfad der XML-Datei für die gespeicherte Aufgabenspezifikation angeben.

Beispiel: Smobackup create -profile Test_profile -full -online -taskSpec „C:\\mirror\\snapmirror.XML“

Das folgende Beispiel zeigt eine Struktur für die Aufgabenspezifikation nach der Verarbeitung, wenn Sie Data ONTAP im 7-Mode verwenden:

```
#     <post-tasks>
#                <task>
#                    <name>Mirror the backup</name>
#                     <description>Mirror the backup</description>
#                </task>
#              <post-tasks>
```

Das folgende Beispiel zeigt eine Struktur für die Aufgabenspezifikation nach der Verarbeitung, wenn Sie Clustered Data ONTAP verwenden:

```
# <task-specification>
#               <post-tasks>
#                   <task>
#                    <name>"Vault the backup for cDOT"</name>
#                     <parameter>
#                     <name>SNAPSHOT_LABEL</name>
#                    <value>TST</value>
#                     </parameter>
#                   </task>
#                 </post-tasks>
#               </task-specification>
#             </preposttask-specification>
```

Verwenden von Aufgabespezifikationen für die Nachbearbeitung, um qtrees zu archivieren

Mit SnapManager für Oracle können Sie das Skript zur Vault der qtrees verwenden, nachdem der Backup-Vorgang in einer Windows Umgebung durchgeführt wurde.

1. Erstellen Sie eine XML-Datei für die Aufgabenspezifikation.
2. Geben Sie in der XML-Datei den Skriptnamen als Eingabeparameter ein.
3. Speichern Sie die XML-Datei für die Aufgabenspezifikation.
4. Erstellen Sie mit dem folgenden Befehl ein geschütztes Backup der Datenbank auf dem sekundären Speicher.

   Beim Erstellen des geschützten Backups müssen Sie nach der Option -taskSpec den vollständigen Pfad der XML-Datei für die gespeicherte Aufgabenspezifikation angeben.

   Beispiel: Smobackup create -profile Test_profile -full -online -taskSpec „C:\\mirror\\snapvault.XML“

Das folgende Beispiel zeigt die Struktur der Aufgabenspezifikation nach der Verarbeitung, wenn Sie Data ONTAP im 7-Mode verwenden:

```
# <post-tasks>
#                 <task>
#                   <name>Vault the backup</name>
#                    <description>Vault the backup</description>
#               </task>
#          <post-tasks>
```

Das folgende Beispiel zeigt die Struktur der Aufgabenspezifikation nach der Verarbeitung, wenn Sie Clustered Data ONTAP verwenden:

```
# <task-specification>
#                 <post-tasks>
#                   <task>
#                    <name>"Vault the backup for cDOT"</name>
#                  <parameter>
#                     <name>SNAPSHOT_LABEL</name>
#                     <value>TST</value>
#                     </parameter>
#                   </task>
#                 </post-tasks>
#               </task-specification>
#             </preposttask-specification>
```

Durchführung von Managementvorgängen

Sie können Managementaufgaben ausführen, nachdem Sie SnapManager eingerichtet und konfiguriert haben. Diese Aufgaben ermöglichen Ihnen das Management des normalen Betriebs, der über Backup, Wiederherstellung und Klonen hinaus geht.

Administratoren können Vorgänge entweder über die grafische Benutzeroberfläche oder über die Befehlszeilenschnittstelle ausführen.

Anzeigen einer Liste von Vorgängen

Sie können eine Zusammenfassung aller Vorgänge anzeigen, die für ein Profil durchgeführt wurden.

Sie können die folgenden Informationen anzeigen, wenn Sie Vorgänge auflisten, die einem bestimmten Profil zugeordnet sind:

- Start- und Enddatum bei Ausführung des Vorgangs
- Betriebsstatus

- Vorgangs-ID
- Art des Vorgangs
- Host, auf dem er ausgeführt wurde

  a. Um die Zusammenfassungsinformationen aller Vorgänge aufzulisten, verwenden Sie den folgenden Befehl: bbs Operation list profile -profile profile_Name-Trennzeichen [-quiet / -verbose]

     Wenn die Option -Trennzeichen angegeben wird, listet der Befehl jede Zeile in einer separaten Zeile auf und die Attribute in dieser Zeile werden durch das angegebene Zeichen getrennt.

Verwandte Informationen

Befehl smo Operation list

Anzeigen von Betriebsdetails

Sie können detaillierte Informationen zu einem bestimmten Profil anzeigen, um den Erfolg oder den Fehler einer Operation zu überprüfen. Zudem können Sie die verwendeten Storage-Ressourcen für einen bestimmten Vorgang ermitteln.

Sie können die folgenden Details zu einer bestimmten Operation anzeigen:

- Vorgangs-ID
- Art des Vorgangs
- Ob die Operation erzwungen wurde
- Laufzeitinformationen, einschließlich Status, Start- und Enddatum des Vorgangs
- Der Host, auf dem der Vorgang ausgeführt wurde, einschließlich der Prozess-ID und der SnapManager-Version
- Repository-Informationen
- Verwendete Storage-Ressourcen

  a. Um die detaillierten Informationen für eine bestimmte Vorgangs-ID anzuzeigen, geben Sie den folgenden Befehl ein: bbs Operation show -profile profile_Name [-Label Label [-id] [-quiet

Verwandte Informationen

Der Befehl smo Operation show

Befehle von einem alternativen Host ausgeben

Sie können CLI-Befehle von einem anderen Host als dem Datenbank-Host ausführen, und SnapManager führt die Befehle durch, die Sie an den entsprechenden Host eingeben.

Damit das System einen Vorgang an den richtigen Host sendet, muss es zunächst wissen, wo das Profil für den Vorgang gefunden werden soll. In diesem Verfahren speichert das System das Profil in Repository-Zuordnungsinformationen für eine Datei im Home-Verzeichnis des Benutzers auf dem lokalen Host.

1. Um das Home-Verzeichnis des lokalen Benutzers auf die Profil-zu-Repository-Zuordnungen aufmerksam zu machen, damit die Operation Request umleiten kann, geben Sie den folgenden Befehl ein: smo-Profil

Sync -Repository-dbname repo_dbname-Host repo_Host-Port repo_Port-Login-username repo_username [-quiet_inverbose]

Überprüfen der SnapManager-Softwareversion

Sie können ermitteln, welche Version des Produkts Sie auf Ihrem lokalen Host ausführen, indem Sie den Versionsbefehl ausführen.

1. Geben Sie zum Überprüfen der SnapManager-Version den folgenden Befehl ein: smo Version

Verwandte Informationen

Der Befehl smo Version

Beenden des SnapManager-Hostservers

Wenn Sie mit SnapManager fertig sind, möchten Sie den Server möglicherweise anhalten.

1. Geben Sie zum Beenden des Servers den folgenden Befehl als Root-Benutzer ein: smo_Server stop

Verwandte Informationen

Der Befehl smo_Server stop

Starten Sie den SnapManager-Hostserver neu

Sie können den SnapManager-Server über das Fenster Dienste neu starten.

1. Klicken Sie Auf **Start** > **Systemsteuerung** > **Verwaltung** > **Services**.
2. Wählen Sie im Fenster Services NetAppSnapManager 3.3 für Oracle aus.
3. Sie können den Server auf eine der folgenden Arten neu starten:
   a. Klicken Sie im linken Bereich auf **Neustart**.
   b. Klicken Sie mit der rechten Maustaste auf NetAppSnapManager 3.3 für Oracle und wählen Sie im Dropdown-Menü die Option **Neustart** aus.
   c. Doppelklicken Sie auf NetAppSnapManager 3.3 für Oracle und klicken Sie im Fenster Eigenschaften auf **Neustart**.

Deinstallieren von SnapManager

Sie können SnapManager vom Host-Server deinstallieren.

- Stoppen Sie den Host-Server, bevor Sie SnapManager deinstallieren.
  a. Klicken Sie auf **Start** > **Systemsteuerung** > **Software hinzufügen oder entfernen**.
  b. Wählen Sie **SnapManager für Oracle**.
  c. Klicken Sie Auf **Deinstallieren**.

Konfigurieren einer E-Mail-Benachrichtigung

Mit SnapManager erhalten Sie eine E-Mail-Benachrichtigung über den Abschlussstatus der von den Profilen ausgeführten Datenbankvorgänge. SnapManager generiert die E-Mail und hilft Ihnen, entsprechend dem Status des Datenbankvorgangs entsprechende Maßnahmen zu ergreifen. Die Konfiguration der E-Mail-Benachrichtigung ist ein optionaler Parameter.

Sie können eine E-Mail-Benachrichtigung für ein einzelnes Profil als Profilbenachrichtigung und für mehrere Profile in einer Repository-Datenbank als zusammenfassende Benachrichtigung konfigurieren.

Profilbenachrichtigung

Für ein individuelles Profil können Sie eine E-Mail für erfolgreiche oder fehlerhafte Datenbankvorgänge erhalten.

Standardmäßig ist die E-Mail-Benachrichtigung für fehlgeschlagene Datenbankvorgänge aktiviert.

Zusammenfassende Benachrichtigung

Mit der Übersichtsbenachrichtigung erhalten Sie eine E-Mail über Datenbankvorgänge, die mit mehreren Profilen durchgeführt werden. Sie können stündliche, tägliche, wöchentliche oder monatliche Benachrichtigungen aktivieren.

Ab SnapManager 3.3 werden zusammenfassende Benachrichtigungen nur dann gesendet, wenn Sie den Hostserver angeben, der die Benachrichtigung senden soll. Wenn Sie SnapManager von einer Version vor 3.3 aktualisieren, werden die zusammenfassenden Benachrichtigungen möglicherweise nicht gesendet, wenn Sie den Host-Server in der Konfiguration für Übersichtsbenachrichtigungen nicht angegeben hatten.

Wenn Sie ein Repository in einem Knoten einer Datenbank erstellen, die sich in einer RAC-Umgebung (Real Application Clusters) befindet und eine zusammenfassende Benachrichtigung aktivieren, wird später, wenn Sie dasselbe Repository einem anderen Knoten der Datenbank hinzufügen, die E-Mail mit der Zusammenfassung zweimal gesendet.

Sie können Benachrichtigungen auf Profilebene oder eine zusammenfassende Benachrichtigung gleichzeitig verwenden.

SnapManager ermöglicht die E-Mail-Benachrichtigung für die folgenden profilausgeführten Datenbankvorgänge:

- Backup auf dem Primärspeicher
- Restore von Backups
- Erstellen von Klonen
- Backup-Überprüfung

Nachdem Sie Profile mit aktivierter E-Mail-Benachrichtigung erstellt oder aktualisiert haben, können Sie sie deaktivieren. Wenn Sie die E-Mail-Benachrichtigung deaktivieren, erhalten Sie für diese profilausgeführten Datenbankvorgänge keine E-Mail-Benachrichtigungen mehr.

Die E-Mail, die Sie erhalten, enthält folgende Details:

- Name des Datenbankvorgangs, z. B. für Backup, Wiederherstellung oder Klonen
- Profilname, der für den Datenbankvorgang verwendet wird
- Name des Hostservers
- Systemkennung der Datenbank
- Start- und Endzeit des Datenbankvorgangs
- Status des Datenbankvorgangs
- Fehlermeldung, falls vorhanden
- Warnmeldungen, falls vorhanden

Sie können Folgendes konfigurieren:

- Mailserver für ein Repository
- E-Mail-Benachrichtigung für ein neues Profil
- E-Mail-Benachrichtigung für ein bestehendes Profil
- Zusammenfassende E-Mail-Benachrichtigung für mehrere Profile unter einem Repository

Sie können die E-Mail-Benachrichtigung sowohl über die Befehlszeilenschnittstelle (CLI) als auch über die grafische Benutzeroberfläche (GUI) konfigurieren.

Konfigurieren eines E-Mail-Servers für ein Repository

Mit SnapManager können Sie die E-Mail-Serverdetails angeben, von denen die E-Mail-Warnungen gesendet werden.

Mit SnapManager können Sie den Hostnamen oder die IP-Adresse des Absenders sowie die Portnummer des E-Mail-Servers für einen Repository-Datenbanknamen angeben, der eine E-Mail-Benachrichtigung erfordert. Sie können die Portnummer des Mail-Servers in einem Bereich von 0 bis 65535 konfigurieren; der Standardwert ist 25. Wenn Sie eine Authentifizierung für die E-Mail-Adresse benötigen, können Sie den Benutzernamen und das Kennwort angeben.

Sie müssen den Namen oder die IP-Adresse des Hostservers angeben, der die E-Mail-Benachrichtigung verarbeitet.

1. Um den E-Mail-Server zum Senden von E-Mail-Warnungen zu konfigurieren, geben Sie folgenden Befehl ein: bbs Notification Set -Sender-emailemail_address-mailhostmailhost-mailportmaiport [-Authentication-usernameusername-passwordpassword] -Repository-portrepo_Port-dbnamerepo_Service_Name -hostrepo_Host-Login-usernamernamerepo_username

   Weitere Optionen für diesen Befehl:

   [-Force]

Gehen Sie wie folgt vor:	Dann…

Um die E-Mail-Adresse des Absenders anzugeben.	Geben Sie die Option -Sender-E-Mail an. Unter SnapManager 3.2 für Oracle können Sie Bindestrich (-) einfügen, während Sie den Domain-Namen der E-Mail-Adresse angeben. Sie können beispielsweise die Absender-E-Mail-Adresse als -sender-emailuser@org-corp.com angeben.
Um den E-Mail-Server-Hostnamen oder die IP-Adresse des Absenders anzugeben.	Geben Sie die Option -mailhost an.
Zur Angabe der Port-Nummer des E-Mail-Servers für einen Repository-Datenbanknamen, der eine E-Mail-Benachrichtigung erfordert. Sie können die Portnummer des Mail-Servers in einem Bereich von null bis 65535 konfigurieren; der Standardwert ist 25.	Geben Sie die Option -mailport an.
Geben Sie den Benutzernamen und das Passwort an, wenn Sie eine Authentifizierung für die E-Mail-Adresse benötigen.	Geben Sie die Option -Authentication an, gefolgt vom Benutzernamen und Passwort.

Im folgenden Beispiel wird der Mail-Server konfiguriert.

```
smo notification set -sender-email admin1@org.com -mailhost
hostname.org.com -mailport 25 authentication -username admin1 -password
admin1 -repository -port 1521 -dbname SMOREPO -host hotspur -login
-username grabal21 -verbose
```

Konfigurieren der E-Mail-Benachrichtigung für ein neues Profil

Wenn Sie ein neues Profil erstellen, können Sie so konfigurieren, dass Sie eine E-Mail-Benachrichtigung nach Abschluss des Datenbankvorgangs erhalten.

- Sie müssen die E-Mail-Adresse konfigurieren, von der die Meldungen gesendet werden.
- Sie müssen eine kommagetrennte Liste für mehrere E-Mail-Adressen verwenden.

  Sie müssen sicherstellen, dass zwischen Komma und der nächsten E-Mail-Adresse kein Leerzeichen vorhanden ist.

  Sie müssen sicherstellen, dass Sie den Satz von E-Mail-Adressen in doppelte Anführungszeichen eingeben.

  a. Geben Sie den folgenden Befehl ein: smo-Profil create -profileprofil [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port -Login-usernamerepo_username_addbnams2 {] [-protourly {-contail} }] [-admgmninto [-associence] [-ademnmninto] [-adressem] [-adressem] [-adressum] [-addnmninto] [-adressum] [-adressum] [-addnmninto] [-adressum] [-commpromnmninct] [-contail] [-commnmnmnmnmgmnmgmnmn.bb] [-adym] [-adymnmnmnmnmnmgmgmn.2] [-contail] [-adym] [-adym

Weitere Optionen für diesen Befehl:

[-Force]

SnapManager unterstützt bis zu 1000 Zeichen für E-Mail-Adressen.

Wenn Sie mithilfe des Profils (zur Erstellung separater Archiv-Log-Backups) eine Sicherung von Datendateien und Archivprotokolldateien erstellen und die Erstellung der Datendatei-Sicherung fehlschlägt, wird die E-Mail-Benachrichtigung mit der Datensicherung als Operationname anstatt Datensicherung und Archivprotokolle als Backup gesendet. Wenn die Datensicherung der Datendatei und der Archivprotokolldatei erfolgreich ist, wird die Ausgabe wie folgt angezeigt:

```
Profile Name    : PROF_31
Operation Name  : Data Backup and Archive Logs Backup
Database SID    : TENDB1
Database Host    : repo1.rtp.org.com
Start Date      : Fri Sep 23 13:37:21 EDT 2011
End Date          : Fri Sep 23 13:45:24 EDT 2011
Status          : SUCCESS
Error messages  :
```

Anpassen des E-Mail-Betreff für ein neues Profil

Sie können den E-Mail-Betreff für das neue Profil anpassen, wenn Sie es erstellen.

Sie können den Betreff der E-Mail mithilfe des {profile}_{Operation-Name}_{db-sid}_{db-Host}_{Startdatum}_{Enddatum}_{Status}-Musters anpassen oder Ihren eigenen Text eingeben.

Variablenname	Beschreibung	Beispielwert
Profil	Profilname, der für den Datenbankvorgang verwendet wird	PROF1
Operation-Name	Name des Datenbankvorgangs	Backup, Daten-Backup, Daten- und Archivprotokolle Backup
db-sid	SID der Datenbank	DB1
db-Host	Name des Hostservers	Hosta
Startdatum	Startzeit der Datenbankoperation im Format mmdd:hh:ss yyyy	April 27 21:00:45 PST 2012
Enddatum	Endzeit des Datenbankvorgangs im Format mmdd:hh:ss yyyy	April 27 21:10:45 PST 2012
Status	Status des Datenbankvorgangs	Erfolg

Wenn Sie keinen Wert für die Variablen angeben, zeigt SnapManager die folgende Fehlermeldung an: Missing value(s) -subject.

1. Geben Sie den folgenden Befehl ein: smo-Profil create -profileprofil [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port-Login -usernamerepo_username_addbnailgms2 [-{ protourly] { [-associence-adressem]} } [-associence [-ademnmnmninto] [-into] [-associmnmailmnmnmnmnmninto] [-into] [-into] [-into [-into] [-into] [-assailmnmaimnmaimninto] [-into] [-commnmaimnmailmnmnmnmnms2] [-adymnmnmnmnmninto] [-adym] [-adym] [-adymnmnmnmninto] [-ady

Konfigurieren der E-Mail-Benachrichtigung für ein vorhandenes Profil

Wenn Sie ein Profil aktualisieren, können Sie so konfigurieren, dass Sie eine E-Mail-Benachrichtigung über den Abschluss des Datenbankvorgangs erhalten.

- Sie müssen die E-Mail-Adresse konfigurieren, von der die Meldungen gesendet werden.
- Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die Benachrichtigungen gesendet werden.

  Sie können eine kommagetrennte Liste für mehrere Adressen verwenden. Sie müssen sicherstellen, dass zwischen Komma und der nächsten E-Mail-Adresse kein Leerzeichen vorhanden ist. Optional können Sie auch einen Betreff zu der E-Mail hinzufügen.

  > Sie müssen sicherstellen, dass Sie den Satz von mehreren E-Mail-Adressen in doppelte Anführungszeichen eingeben.

  a. Geben Sie den folgenden Befehl ein:smo-Profil-Update -profilprofil [-profile-passwordprofile_password][-Database-dbnamedb_dbname-Host db_Host [-siddb_sid] [-Login -usernamedb_username-password_password [{{ {}}}-Login] [-dbnamens2_username-password_adressum] [-dmin] [-commentnestem] [-commend] [-commend] [-commend] [-dmnestamness2] [-comm] [-commend] [-[-] [-] [-] [-] [-] [-dnesson] [-] [-] [-dnesson] [-commodnesson] [-comm] [-commend] [-] [-commend] [-] [-jur] [-comments2] [-comments2] [-jur] [-jur] [-comm] [

     Mit der Option Erfolg erhalten Sie nur eine Benachrichtigung für erfolgreiche Datenbankvorgänge und die Ausfalloption, eine Benachrichtigung nur für fehlerhafte Datenbankvorgänge zu erhalten.

Anpassen des E-Mail-Betreff für ein vorhandenes Profil

SnapManager ermöglicht Ihnen, das Muster des E-Mail-Betreff für ein bestehendes Profil anzupassen, indem Sie dieses Profil aktualisieren. Dieses benutzerdefinierte Muster für Studienteilnehmer gilt nur für das aktualisierte Profil.

1. Geben Sie den folgenden Befehl ein: smo-Profil-Update -profilprofil [-profile-passwordprofile_password][-Database-dbnamedb_dbname-Host db_Host [-siddb_sid] [-Login -usernamedb_username-adress1 [-{ dmails2] [-{ jur] [-{ commentail}}}-[-] [-] [-]]-assourly [-commentail] [-] [-] [-]] [-commentail-] [-] [-] [-] [-]]] [-] [-]]] [-]] [-]] [-]]]] [-associmundintourly-associmnmailmnesson-[-[-[-[-commn.m] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-] [-]]] [-] [-]

Konfigurieren einer E-Mail-Benachrichtigung mit Zusammenfassung für mehrere Profile

Mit SnapManager können Sie eine E-Mail-Benachrichtigung für mehrere Profile unter einer Repository-Datenbank konfigurieren.

Sie können den SnapManager-Server-Host als Benachrichtigungs-Host festlegen, von dem aus die zusammenfassende Benachrichtigung E-Mail an die Empfänger gesendet wird. Wenn der Hostname oder die IP-Adresse des SnapManager-Servers geändert wird, kann auch der Benachrichtigungs-Host aktualisiert werden.

Sie können eine der Zeitplanzeiten auswählen, zu denen Sie eine E-Mail-Benachrichtigung benötigen:

- Stündlich: Um jede Stunde eine E-Mail-Benachrichtigung zu erhalten
- Täglich: Um täglich eine E-Mail-Benachrichtigung zu erhalten
- Wöchentlich: Um wöchentlich eine E-Mail-Benachrichtigung zu erhalten
- Monatlich: Um monatlich eine E-Mail-Benachrichtigung zu erhalten

Sie müssen eine einzelne E-Mail-Adresse oder eine kommagetrennte Liste von E-Mail-Adressen eingeben, um Benachrichtigungen für Vorgänge zu erhalten, die mit diesen Profilen durchgeführt werden. Wenn Sie mehrere E-Mail-Adressen eingeben, müssen Sie sicherstellen, dass zwischen Komma und der nächsten E-Mail-Adresse kein Leerzeichen vorhanden ist.

Sie müssen sicherstellen, dass Sie den Satz von mehreren E-Mail-Adressen in doppelte Anführungszeichen eingeben.

SnapManager ermöglicht Ihnen das Hinzufügen eines benutzerdefinierten E-Mail-Betreff unter Verwendung der folgenden Variablen:

- Profilname, der für den Datenbankvorgang verwendet wird.
- Datenbankname
- SID der Datenbank
- Name des Hostservers
- Startzeit des Datenbankvorgangs im Format yyyymmdd:hh:ss
- Endzeit des Datenbankvorgangs im Format yyyyymmdd:hh:ss
- Status des Datenbankvorgangs

Wenn Sie kein angepasstes Thema hinzufügen möchten, zeigt SnapManager eine Fehlermeldung an: Missing value -subject.

1. Geben Sie folgenden Befehl ein: bbs Notification Update-summary-notification -Repository-portrepo_Port -dbnamerepo_Service_Name-hotropo_Host-Login-usernamerepo_username -emailemail_address1,email_address2-subject-pattern-frequency {-Daily-timedaily-time {4 7-31 5-3 6-protagel1} {}} 1-wöchentlicher Hinweis

   Weitere Optionen für diesen Befehl:

   [-Force] [-noprompt]

```
smo notification update-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5 –email-address
admin@org.com –subject success –frequency -daily -time 19:30:45
–profiles sales1 -notification-host wales
```

Hinzufügen eines neuen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung

Nachdem Sie eine E-Mail-Benachrichtigung für die Repository-Datenbank konfiguriert haben, können Sie mithilfe des Befehls Summary Notification ein neues Profil zur zusammenfassenden Benachrichtigung hinzufügen.

1. Geben Sie den folgenden Befehl ein: smo-Profil create -profileprofile_Name [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port-Login -usernamerepo_username_countnmprop [-countnum] [-commodnmgmgmn.jmgmgm.j-injur [-] [-assourly [-assound] [-countgmsnmnmgmnmnmnmnmgame] [-] [-jm] [-assumb] [-assourly-datamnmnmn.jmn.jmnmn.jmnmn.jmgmgmgmgmsdn.jur] [-{] [-{] [-datamnmn.jurly-} }] [-datamnmnmnmnm.jmnm.jmn.jmnm

   Weitere Optionen für diesen Befehl:

   [-Force]

Hinzufügen eines vorhandenen Profils zu E-Mail-Benachrichtigungen mit Zusammenfassung

Mit SnapManager können Sie ein vorhandenes Profil zu einer zusammengefassten E-Mail-Benachrichtigung hinzufügen und das Profil aktualisieren.

1. Geben Sie den folgenden Befehl ein: smo-Profil-Update -profilprofile_Name [-profile-passwordprofile_password] -Repository-dbnamerepo_Service_Name-hostrepo_Host-portrepo_Port-Login -usernamerepo_username_countnmpropery-{ Name [{-countnmnum} }] [-countngmgmsdnum] [-adname] [-countgmnmnmnmgmgmnmb] [-adym] [-adname] [-adymnm.jm.jm.jm.jm.jm.jm.j.jmgmgmgm.jm.jmgm.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j

Deaktivieren der E-Mail-Benachrichtigung für mehrere Profile

Nachdem Sie die E-Mail-Benachrichtigung für mehrere Profile aktiviert haben, können Sie sie deaktivieren, dass sie keine E-Mail-Benachrichtigungen mehr erhalten.

Mit SnapManager können Sie die E-Mail-Benachrichtigung mit der Zusammenfassung für diese profilausgeführten Datenbankvorgänge deaktivieren. Geben Sie über die SnapManager-CLI den Befehl Benachrichtigung remove-summary-notification ein, um die Zusammenfassung der E-Mail-Benachrichtigung für mehrere Profile und den Namen der Repository-Datenbank zu deaktivieren, für die Sie keine E-Mail-Benachrichtigung benötigen.

1. Um die zusammenfassende Benachrichtigung für mehrere Profile in einer Repository-Datenbank zu deaktivieren, geben Sie den folgenden Befehl ein: smo notification remove-summary-notification -Repository-portrepo_Port-dbnamerepo_Service_Name-hostrepo_Host-Login-usernamerepo_username

Das folgende Beispiel zeigt, dass die zusammenfassende Benachrichtigung für mehrere Profile in einer Repository-Datenbank deaktiviert wird:

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5
```

Erstellen von Aufgabenspezifikationsdatei und Skripten für SnapManager-Vorgänge

SnapManager für Oracle verwendet eine XML-Datei (Extensible Markup Language) für die Aufgabenspezifikation, die Voraufgaben und Nachaufgaben für die Backup-, Wiederherstellungs- und Klonvorgänge anzeigt. Sie können die Skriptnamen vor und nach der Aufgabe in die XML-Datei einfügen, damit die Aufgaben vor oder nach den Backup-, Wiederherstellungs- und Klonvorgängen ausgeführt werden.

In SnapManager (3.1 oder früher) können Sie die Skripte für Voraufgabe und Nachaufgaben nur für den Klonvorgang ausführen. In SnapManager (3.2 oder höher) für Oracle können Sie die Pre- und Post-Task-Skripte für Backup-, Restore- und Klonvorgänge ausführen.

In SnapManager (3.1 oder früher) ist der Abschnitt für die Aufgabenspezifikation Teil der XML-Datei für die Klonspezifikation. Aus SnapManager 3.2 für Oracle ist der Abschnitt „Aufgabenspezifikation“ eine separate XML-Datei.

SnapManager 3.3 oder höher unterstützt nicht die Verwendung der XML-Datei für die Klonspezifikation, die in den Versionen vor SnapManager 3.2 erstellt wurde.

In SnapManager (3.2 oder höher) für Oracle müssen Sie sicherstellen, dass die folgenden Voraussetzungen für einen erfolgreichen SnapManager-Betrieb erfüllt sind:

- Verwenden Sie für Sicherungs- und Wiederherstellungsvorgänge die XML-Datei für die Aufgabenspezifikation.
- Geben Sie für den Klonvorgang zwei Spezifikationsdateien an: Eine XML-Datei für die Klonspezifikation und eine XML-Datei für die Aufgabenspezifikation.

  Wenn Sie Voraufgaben oder Nachaufgaben aktivieren möchten, können Sie optional die XML-Datei für die Aufgabenspezifikation hinzufügen.

Sie können die Aufgabenspezifikationsdatei über die grafische Benutzeroberfläche (GUI) von SnapManager, die Befehlszeilenschnittstelle (CLI) oder einen Texteditor erstellen. Sie müssen eine Erweiterung .XML verwenden, damit die Datei entsprechende Bearbeitungsfunktionen ermöglicht. Vielleicht möchten Sie diese Datei speichern, damit Sie sie für zukünftige Backup-, Restore- und Klonvorgänge verwenden können.

Die XML-Datei für die Aufgabenspezifikation enthält zwei Abschnitte:

- Der Abschnitt „Voraufgaben“ enthält Skripte, die vor Backup-, Wiederherstellungs- und Klonvorgängen ausgeführt werden können.
- Der Abschnitt „Aufgaben nach“ enthält Skripte, die nach Backup-, Restore- und Klonvorgängen ausgeführt werden können.

Die Werte, die in den Abschnitten vor und nach Aufgaben enthalten sind, müssen den folgenden Richtlinien entsprechen:

- Aufgabenname: Der Name der Aufgabe muss mit dem Namen des Skripts übereinstimmen, das bei der Ausführung des Befehls plugin.sh -beschreibe angezeigt wird.

  Wenn eine Diskrepanz besteht, erhalten Sie möglicherweise die folgende Fehlermeldung: Die Datei wurde nicht gefunden.

- Parametername: Der Name des Parameters muss ein String sein, der als Umgebungsvariable-Einstellung verwendet werden kann.

  Die Zeichenfolge muss mit dem Parameternamen im benutzerdefinierten Skript übereinstimmen, das bei der Ausführung des Befehls plugin.sh -beschreibe angezeigt wird.

Sie können die Spezifikationsdatei basierend auf der Struktur der folgenden Beispielaufgabe Spezifikationsdatei erstellen:

```
<task-specification>
  <pre-tasks>
<task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </post-tasks>
</task-specification>
```

Die XML-Datei für die Aufgabenspezifikation darf keine Richtlinien enthalten.

Über die SnapManager-Benutzeroberfläche können Sie den Parameterwert festlegen und die XML-Datei speichern. Sie können die Seite „Task Enabling“ des Assistenten „Backup Create“, „Restore“ oder „Recovery“ und „Clone Create“ verwenden, um die vorhandene XML-Datei für die Aufgabenspezifikation zu laden und die ausgewählte Datei für die Voraufgabe oder die Nachbearbeitung zu verwenden.

Eine Aufgabe kann mehrfach ausgeführt werden, entweder mit den gleichen oder mit unterschiedlichen Parameter- und Wertkombinationen. Zum Beispiel können Sie eine Aufgabe Speichern verwenden, um

mehrere Dateien zu speichern.

SnapManager verwendet die in der Aufgabenspezifikationsdatei angegebenen XML-Tags für die Vorverarbeitung oder Nachbearbeitung der Backup-, Wiederherstellungs- und Klonvorgänge unabhängig von der Dateierweiterung der Aufgabenspezifikationsdatei.

Erstellen von vor-, Post-Task- und Richtlinienskripten

SnapManager ermöglicht das Erstellen von Skripten für die Vorverarbeitung, die Nachbearbeitung und die Richtlinienaufgaben für Backup, Wiederherstellung und Klonvorgänge. Sie müssen die Skripte in das richtige Installationsverzeichnis platzieren, um die Vorverarbeitung, die Nachbearbeitungsaktivität und die Richtlinienaufgaben des SnapManager-Vorgangs auszuführen.

Skriptinhalt vor und nach der Aufgabe

Alle Skripte müssen Folgendes enthalten:

- Spezifische Vorgänge (prüfen, beschreiben und ausführen)
- (Optional) vordefinierte Umgebungsvariablen
- Spezifischer Fehlercode (Rückgabecode (rc))

Sie müssen den korrekten Code für die Fehlerbehandlung angeben, um das Skript zu validieren.

Sie können die Vortaskskripte für viele Zwecke verwenden, zum Beispiel, um einen Festplattenspeicher vor dem Start des SnapManager-Vorgangs zu bereinigen. So können Sie beispielsweise auch die Skripts für die Nachbearbeitung verwenden, um einschätzen zu können, ob SnapManager über genügend Festplattenspeicher verfügt, um den Vorgang abzuschließen.

Policy Task Skript Inhalt

Sie können das Richtlinienskript ausführen, ohne bestimmte Aufgaben wie das Prüfen, Beschreiben und Ausführen von auszuführen. Das Skript enthält die vordefinierten Umgebungsvariablen (optional) und den spezifischen Code zur Fehlerbehandlung.

Das Richtlinienskript wird vor der Backup-, Wiederherstellungs- und Klonvorgänge ausgeführt.

- Unterstützte Formate*

Als Prescript und Post-Script kann eine Befehlsdatei mit Erweiterung .cmd verwendet werden.

Wenn Sie die Shell-Skriptdatei auswählen, antwortet der SnapManager-Vorgang nicht. Um dies zu beheben, müssen Sie die Befehlsdatei im Plug-in-Verzeichnis angeben und den SnapManager-Vorgang erneut ausführen.

Skript-Installationsverzeichnis

Das Verzeichnis, in dem Sie das Skript installieren, beeinflusst die Verwendung. Sie können die Skripte in das Verzeichnis platzieren und das Skript ausführen, bevor oder nach dem Backup-, Wiederherstellungs- oder Klonvorgang erfolgt. Sie müssen das Skript in das in der Tabelle angegebene Verzeichnis legen und es auf

optionaler Basis verwenden, wenn Sie den Backup-, Wiederherstellungs- oder Klonvorgang angeben.

Sie müssen sicherstellen, dass das Plugin-Verzeichnis die ausführbare Berechtigung hat, bevor Sie die Skripte für den SnapManager-Betrieb verwenden.

Aktivität	Backup	Wiederherstellen	Klon
Vorverarbeitung	<default_Installation_Directory>\Plugins\Backup\create\pre	<default_Installation_Directory>\Plugins\restore\create\pre	<default_Installation_Directory>\Plugins\Clone\create\pre
Nachbearbeitet	<default_Installation_Directory>\Plugins\Backup\create\post	<default_Installation_Directory>\Plugins\restore\create\post	<default_Installation_Directory>\Plugins\Clone\create\post
Richtlinienbasiert	<default_Installation_Directory>\Plugins\Backup\create\Policy	<default_Installation_Directory>\Plugins\restore\create\Policy	<default_Installation_Directory>\Plugins\Clone\create\Policy

Sample scripts Position

Im Folgenden sind einige Beispiele für die Skripte vor und nach der Aufgabe für die Backup- und Klonvorgänge aufgeführt, die im Installationspfad verfügbar sind:

- <default_Installation_Directory>\Plugins\Beispiele\Backup\create\pre
- <default_Installation_Directory>\Plugins\Beispiele\Backup\create\post
- <default_Installation_Directory>\Plugins\Beispiele\Clone\create\pre
- <default_Installation_Directory>\Plugins\Beispiele\Clone\create\post

Was Sie im Skript ändern können

Wenn Sie ein neues Skript erstellen, können Sie nur die Operationen beschreiben und ausführen ändern. Jedes Skript muss die folgenden Variablen enthalten: Kontext, Timeout und Parameter.

Die Variablen, die Sie in der Beschreiben-Funktion des Skripts beschrieben haben, müssen zu Beginn des Skripts deklariert werden. Sie können neue Parameterwerte in Parameter=() hinzufügen und dann die Parameter in der Funktion Ausführen verwenden.

Beispielskript

Im Folgenden ist ein Beispielskript mit einem vom Benutzer angegebenen Rückgabecode zur Schätzung des Speicherplatzes im SnapManager-Host:

```
@echo off
REM $Id:
//depot/prod/capstan/Rcapstan_ganges/src/plugins/windows/examples/clone/cr
eate/policy/validate_sid.cmd#1 $
REM $Revision: #1 $ $Date: 2011/12/06 $
REM
```

```
REM

set /a EXIT=0

set name="Validate SID"
set description="Validate SID used on the target system"
set parameter=()

rem reserved system IDs
set INVALID_SIDS=("ADD" "ALL" "AND" "ANY" "ASC" "COM" "DBA" "END" "EPS"
"FOR" "GID" "IBM" "INT" "KEY" "LOG" "MON" "NIX" "NOT" "OFF" "OMS" "RAW"
"ROW" "SAP" "SET" "SGA" "SHG" "SID" "SQL" "SYS" "TMP" "UID" "USR" "VAR")

if /i "%1" == "-check" goto :check
if /i "%1" == "-execute" goto :execute
if /i "%1" == "-describe" goto :describe

:usage:
    echo usage: %0 "{ -check | -describe | -execute }"
    set /a EXIT=99
    goto :exit

:check
    set /a EXIT=0
    goto :exit

:describe
    echo SM_PI_NAME:%name%
    echo SM_PI_DESCRIPTION:%description%
    set /a EXIT=0
    goto :exit

:execute
    set /a EXIT=0

    rem SM_TARGET_SID must be set
    if "%SM_TARGET_SID%" == "" (
        set /a EXIT=4
        echo SM_TARGET_SID not set
        goto :exit
    )

    rem exactly three alphanumeric characters, with starting with a letter
    echo %SM_TARGET_SID% | findstr "\<[a-zA-Z][a-zA-Z0-9][a-zA-Z0-9]\>"
>nul
    if %ERRORLEVEL% == 1 (
        set /a EXIT=4
```

```
        echo SID is defined as a 3 digit value starting with a letter.
[%SM_TARGET_SID%] is not valid.
        goto :exit
    )

    rem not a SAP reserved SID
    echo %INVALID_SIDS% | findstr /i \"%SM_TARGET_SID%\" >nul
    if %ERRORLEVEL% == 0 (
        set /a EXIT=4
        echo SID [%SM_TARGET_SID%] is reserved by SAP
        goto :exit
    )

    goto :exit



:exit
    echo Command complete.
    exit /b %EXIT%
```

Vorgänge in Taskskripten

Die von Ihnen erstellten Pre-Task- oder Post-Task-Skripte müssen einer Standard-Plug-in-Struktur von SnapManager für Oracle entsprechen.

Die vor- und Nachaufgaben-Skripte müssen die folgenden Vorgänge umfassen:

- Prüfen
- Beschreiben
- Ausführen

Wenn einer dieser Vorgänge nicht im Skript für die Aufgabe vor oder nach der Aufgabe angegeben ist, wird das Skript ungültig.

Wenn Sie den smo Plugin Check Befehl für die Pre-Task oder Post-Task-Skripte ausführen, zeigt der zurückgegebene Status der Skripte Fehler an (da der zurückgegebene Statuswert nicht Null ist).

Betrieb	Beschreibung
Prüfen	Der SnapManager-Server führt den Befehl plugin.sh -Check aus, um sicherzustellen, dass das System über die Ausführungsberechtigung auf den Plug-in-Skripten verfügt. Sie können auch die Überprüfung der Dateiberechtigungen auf dem Remote-System einschließen.

Beschreiben	Auf dem SnapManager-Server wird der Befehl plugin.sh -beschreibe ausgeführt, um Informationen über Ihr Skript abzurufen und die von der Spezifikationsdatei bereitgestellten Elemente zu entsprechen. Ihr Plug-in-Skript muss die folgenden Beschreibungen enthalten:
	• SM_PI_NAME: Skriptname. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_DESCRIPTION: Beschreibung des Zwecks des Skripts. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_CONTEXT: Kontext, in dem das Skript ausgeführt werden soll, zum Beispiel root oder oracle. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_TIMEOUT: Die maximale Zeit (in Millisekunden), die SnapManager warten sollte, bis das Skript die Verarbeitung beendet und die Ausführung beendet. Sie müssen für diesen Parameter einen Wert angeben.
	• SM_PI_PARAMETER: Ein oder mehrere benutzerdefinierte Parameter, die für die Verarbeitung Ihres Plug-in-Skripts erforderlich sind. Jeder Parameter sollte in einer neuen Ausgabezeile aufgeführt werden und den Namen des Parameters sowie eine Beschreibung enthalten. Wenn das Skript die Verarbeitung abgeschlossen hat, wird Ihrem Skript der Parameterwert durch eine Umgebungsvariable zur Verfügung gestellt.
	Im Folgenden finden Sie eine Beispielausgabe des Skripts Followup_Aktivitäten.
	`plugin.sh - describe`
	
	`SM_PI_NAME:Followup_activities`
	`SM_PI_DESCRIPTION:this script contains follow-up activities to be executed after the clone create operation.`
	`SM_PI_CONTEXT:root`
	`SM_PI_TIMEOUT:60000`
	`SM_PI_PARAMETER:SCHEMAOWNER:Name of the database schema owner.`
	`Command complete.`

Ausführen	Der SnapManager-Server führt den Befehl plugin.sh -execute aus, um Ihr Skript zur Ausführung des Skripts zu starten.

Variablen, die in den Taskskripten für den Backup-Vorgang verfügbar sind

SnapManager stellt Kontextinformationen in Form von Umgebungsvariablen für den durchzuführenden Backup-Vorgang zur Verfügung. Ihr Skript kann beispielsweise den Namen des ursprünglichen Hosts, den Namen der Aufbewahrungsrichtlinie und das Etikett des Backups abrufen.

In der folgenden Tabelle sind die Umgebungsvariablen aufgeführt, die Sie in Ihren Skripten verwenden können:

Variablen	Beschreibung	Formatieren
SM_OPERATION_ID	Gibt die ID des aktuellen Vorgangs an	Zeichenfolge
SM_PROFILE_NAME	Gibt den Namen des verwendeten Profils an	Zeichenfolge
SM_SID	Gibt die Systemkennung der Datenbank an	Zeichenfolge
SM_HOST	Gibt den Hostnamen der Datenbank an	Zeichenfolge
SM_OS_USER	Gibt den Betriebssystemeigentümer der Datenbank an	Zeichenfolge
SM_OS_GROUP	Gibt die Betriebssystemgruppe der Datenbank an	Zeichenfolge
SM_BACKUP_TYP	Gibt den Typ des Backups an (online, offline oder Auto)	Zeichenfolge
SM_BACKUP_LABEL	Gibt die Bezeichnung des Backups an	Zeichenfolge
SM_BACKUP_ID	Gibt die ID des Backups an	Zeichenfolge
SM_BACKUP_RETENTION	Gibt den Aufbewahrungszeitraum an	Zeichenfolge
SM_BACKUP_PROFIL	Gibt das Profil an, das für dieses Backup verwendet wird	Zeichenfolge

SM_ALLOW_DATABASE_SHUTDOWN	Gibt an, ob Sie die Datenbank starten oder herunterfahren möchten Wenn erforderlich, können Sie die Option -Force über die Befehlszeilenschnittstelle verwenden.	boolesch
SM_BACKUP_UMFANG	Gibt den Umfang des Backups an (vollständig oder teilweise)	Zeichenfolge
SM_TARGET_FILER_NAME	Gibt den Namen des Zielspeichersystems an **Hinweis:** Wenn mehr als ein Speichersystem verwendet wird, müssen die Namen des Speichersystems durch Kommas getrennt werden.	Zeichenfolge
SM_TARGET_VOLUME_NAME	Gibt den Namen des Zielvolume an **Hinweis:** der Name des Zielvolumes muss mit dem Namen des Speichergeräts vorbestimmt sein, zum Beispiel SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	Zeichenfolge
SM_HOST_FILE_SYSTEM	Gibt das Host-Dateisystem an	Zeichenfolge
SM_SNAPSHOT_NAMEN	Gibt die Snapshot-Liste an **Hinweis:** der Name der Snapshot-Kopien muss mit dem Namen des Storage-Systems und dem Volume-Namen vorangestellt sein. Die Namen der Snapshot Kopien werden durch Kommata getrennt.	String-Array
SM_ARCHIVE_LOGS_DIRECTORY	Gibt das Verzeichnis der Archivprotokolle an **Hinweis:** Wenn sich die Archivprotokolle in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_REDO_LOGS_DIRECTORY	Gibt das Verzeichnis der Redo-Logs an **Hinweis:** Wenn sich die Redo-Logs in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array

SM_CONTROL_FILES_DIRECTORY	Gibt das Verzeichnis der Steuerdateien an **Hinweis:** Wenn sich die Steuerdateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_DATA_FILES_DIRECTORY	Gibt das Verzeichnis der Datendateien an **Hinweis:** Wenn sich die Datendateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
Benutzerdefiniert	Gibt zusätzliche Parameter an, die vom Benutzer definiert werden. Benutzerdefinierte Parameter sind für Plug-ins, die als Richtlinien verwendet werden, nicht verfügbar.	Benutzerdefiniert

Variablen, die in den Taskskripten für den Wiederherstellungsvorgang verfügbar sind

SnapManager stellt Kontextinformationen in Form von Umgebungsvariablen für den durchgeführten Wiederherstellungsvorgang bereit. Ihr Skript kann beispielsweise den Namen des ursprünglichen Hosts und die Bezeichnung des wiederhergestellten Backups abrufen.

In der folgenden Tabelle sind die Umgebungsvariablen aufgeführt, die Sie in Ihren Skripten verwenden können:

Variablen	Beschreibung	Formatieren
SM_OPERATION_ID	Gibt die ID des aktuellen Vorgangs an	Zeichenfolge
SM_PROFILE_NAME	Gibt den Namen des verwendeten Profils an	Zeichenfolge
SM_HOST	Gibt den Hostnamen der Datenbank an	Zeichenfolge
SM_OS_USER	Gibt den Betriebssystemeigentümer der Datenbank an	Zeichenfolge
SM_OS_GROUP	Gibt die Betriebssystemgruppe der Datenbank an	Zeichenfolge

Variablen	Beschreibung	Formatieren
SM_BACKUP_TYP	Gibt den Typ des Backups an (online, offline oder Auto)	Zeichenfolge
SM_BACKUP_LABEL	Gibt die Sicherungsbezeichnung an	Zeichenfolge
SM_BACKUP_ID	Gibt die Backup-ID an	Zeichenfolge
SM_BACKUP_PROFIL	Gibt das Profil an, das für die Sicherung verwendet wird	Zeichenfolge
SM_RECOVERY_TYPE	Gibt die Informationen zur Wiederherstellungskonfiguration an	Zeichenfolge
SM_VOLUME_RESTORE_MODE	Gibt die Wiederherstellungskonfiguration des Volumes an	Zeichenfolge
SM_TARGET_FILER_NAME	Gibt den Namen des Zielspeichersystems an **Hinweis:** Wenn mehr als ein Speichersystem verwendet wird, müssen die Namen des Speichersystems durch Kommas getrennt werden.	Zeichenfolge
SM_TARGET_VOLUME_NAME	Gibt den Namen des Zielvolume an **Hinweis:** der Name des Zielvolumes muss mit dem Namen des Speichergeräts vorbestimmt sein, zum Beispiel SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.	Zeichenfolge
SM_HOST_FILE_SYSTEM	Gibt das Host-Dateisystem an	Zeichenfolge
SM_SNAPSHOT_NAMEN	Gibt die Snapshot-Liste an **Hinweis:** der Name der Snapshot-Kopien muss mit dem Namen des Storage-Systems und dem Volume-Namen vorangestellt sein. Die Namen der Snapshot Kopien werden durch Kommata getrennt.	String-Array

Variablen	Beschreibung	Formatieren
SM_ARCHIVE_LOGS_DIRECTORY	Gibt das Verzeichnis der Archivprotokolle an **Hinweis:** Wenn sich die Archivprotokolle in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_REDO_LOGS_DIRECTORY	Gibt das Verzeichnis der Redo-Logs an **Hinweis:** Wenn sich die Redo-Logs in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_CONTROL_FILES_DIRECTORY	Gibt das Verzeichnis der Steuerdateien an **Hinweis:** Wenn sich die Steuerdateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array
SM_DATA_FILES_DIRECTORY	Gibt das Verzeichnis der Datendateien an **Hinweis:** Wenn sich die Datendateien in mehr als einem Verzeichnis befinden, werden die Namen dieser Verzeichnisse durch Kommas getrennt.	String-Array

In den Aufgabenskripten verfügbare Variablen für den Klonvorgang

SnapManager stellt Kontextinformationen in Form von Umgebungsvariablen für den ausgeführten Klonvorgang bereit. Ihr Skript kann beispielsweise den Namen des ursprünglichen Hosts, den Namen der Klondatenbank und den Namen des Backups abrufen.

In der folgenden Tabelle sind die Umgebungsvariablen aufgeführt, die Sie in Ihren Skripten verwenden können:

Variablen	Beschreibung	Formatieren
SM_ORIGINAL_SID	SID der ursprünglichen Datenbank	Zeichenfolge
SM_URSPRÜNGLICHER_HOST	Der ursprünglichen Datenbank zugeordnete Hostname	Zeichenfolge

SM_ORIGINAL_OS_USER	OS-Eigentümer der ursprünglichen Datenbank	Zeichenfolge
SM_ORIGINAL_OS_GROUP	OS-Gruppe der ursprünglichen Datenbank	Zeichenfolge
SM_TARGET_SID	SID der Klondatenbank	Zeichenfolge
SM_TARGET_HOST	Der Klondatenbank zugeordnete Host-Name	Zeichenfolge
SM_TARGET_OS_USER	OS-Eigentümer der Klondatenbank	Zeichenfolge
SM_TARGET_OS_GROUP	OS-Gruppe der Klondatenbank	Zeichenfolge
SM_TARGET_DB_PORT	Port der Zieldatenbank	Ganzzahl
SM_TARGET_GLOBAL_DB_NAME	Globaler Datenbankname der Zieldatenbank	Zeichenfolge
SM_BACKUP_LABEL	Bezeichnung des für den Klon verwendeten Backups	Zeichenfolge

Fehlerbehandlung in benutzerdefinierten Skripts

SnapManager verarbeitet das benutzerdefinierte Skript auf Basis der jeweiligen Rückgabecodes. Wenn Ihr benutzerdefiniertes Skript beispielsweise den Wert 0, 1, 2 oder 3 zurückgibt, wird der Klonprozess von SnapManager fortgesetzt. Der Rückgabecode beeinflusst auch die Prozesse von SnapManager und gibt die Standardausgabe Ihrer Skriptausführung zurück.

Rückgabecode	Beschreibung	Fahren Sie mit der Verarbeitung des Vorgangs fort
0	Das Skript wurde erfolgreich abgeschlossen.	Ja.
1	Das Skript wurde erfolgreich mit Informationsmeldungen abgeschlossen.	Ja.
2	Das Skript wurde abgeschlossen, enthält jedoch Warnungen	Ja.
3	Das Skript schlägt fehl, der Vorgang wird jedoch fortgesetzt.	Ja.

4 oder >4	Das Skript schlägt fehl, und der Vorgang wird beendet.	Nein

Anzeigen von Beispielskripten für das Plug-in

SnapManager enthält Skripte, die Sie als Beispiele dafür verwenden können, wie Sie Ihre eigenen Skripte oder als Grundlage für Ihre benutzerdefinierten Skripts erstellen.

Die Beispielskripts für das Plug-in finden Sie unter folgender Adresse:

- <default_install_Directory>\Plugins\Beispiele\Backup\create
- <default_install_Directory>\Plugins\Beispiele\Clone\create
- <default_install_Directory>\Plugins\Windows\Beispiele\Backup\create\post

Das Verzeichnis, das die Beispiel-Plug-in-Skripte enthält, umfasst die folgenden Unterverzeichnisse:

- Richtlinie: Enthält Skripte, die, wenn sie konfiguriert sind, immer im Klonvorgang ausgeführt werden.
- Pre: Enthält Skripte, die, wenn konfiguriert, vor dem Klonvorgang ausgeführt werden.
- Post: Enthält Skripte, die, wenn sie konfiguriert sind, nach dem Klonvorgang ausgeführt werden.

Die folgende Tabelle beschreibt die Beispielskripts:

Skriptname	Beschreibung	Skripttyp
validate_sid.sh	Enthält zusätzliche Prüfungen für den auf dem Zielsystem verwendeten SID. Das Skript überprüft, ob der SID die folgenden Eigenschaften hat: • Enthält drei alphanumerische Zeichen • Beginnt mit einem Buchstaben	Richtlinie
cleanup.sh	Reinigt das Zielsystem, so dass es bereit ist, den neu erstellten Klon zu speichern. Speichert oder löscht Dateien und Verzeichnisse je nach Bedarf.	Voraufgabe
Mirror_the_Backup.cmd	Spiegelung der Volumes nach Ausführung des Backups in einer Windows-Umgebung bei Verwendung von Data ONTAP im 7-Mode	Aufgabe einstellen

Vault_the_Backup.cmd	Vaults die qtrees, nachdem die Backups in einer Windows Umgebung durchgeführt werden, wenn sie entweder Data ONTAP 7-Mode verwenden.	Aufgabe einstellen
Mirror_the_Backup_cDOT.cmd	Spiegelung der Volumes nach dem Backup-Vorgang in einer Windows Umgebung bei Verwendung von Clustered Data ONTAP	Aufgabe einstellen
Vault_the_Backup_cDOT.cmd	Vaults die qtrees, nachdem der Backup-Vorgang in einer Windows Umgebung durchgeführt wird, wenn Sie Clustered Data ONTAP verwenden.	Aufgabe einstellen

Mit SnapManager gelieferte Skripte verwenden standardmäßig die BASH Shell. Sie müssen sicherstellen, dass die Unterstützung für DIE BASH-Shell auf Ihrem Betriebssystem installiert ist, bevor Sie versuchen, einen der Beispielskripte auszuführen.

1. Um zu überprüfen, ob Sie die BASH-Shell verwenden, geben Sie den folgenden Befehl an der Eingabeaufforderung ein: Bash

   Wenn kein Fehler auftritt, funktioniert DIE BASH-Shell ordnungsgemäß.

   Sie können alternativ den Befehl which-bash an der Eingabeaufforderung eingeben.

2. Suchen Sie das Skript im folgenden Verzeichnis:

   <installdir>\Plugins\Beispiele\Clone\create

3. Öffnen Sie das Skript in einem Skript-Editor wie vi.

Beispielskript

Das folgende benutzerdefinierte Beispielskript validiert die Namen der Datenbank-SID und verhindert, dass ungültige Namen in der geklonten Datenbank verwendet werden. Es umfasst drei Operationen (prüfen, beschreiben und ausführen), die aufgerufen werden, nachdem Sie das Skript ausgeführt haben. Das Skript enthält auch Fehlermeldungs-Handling mit den Codes 0, 4 und >4.

```
@echo off
REM $Id:
//depot/prod/capstan/Rcapstan_ganges/src/plugins/windows/examples/clone/cr
eate/policy/validate_sid.cmd#1 $
REM $Revision: #1 $ $Date: 2011/12/06 $
REM
REM

set /a EXIT=0
```

```
set name="Validate SID"
set description="Validate SID used on the target system"
set parameter=()

rem reserved system IDs
set INVALID_SIDS=("ADD" "ALL" "AND" "ANY" "ASC" "COM" "DBA" "END" "EPS"
"FOR" "GID" "IBM" "INT" "KEY" "LOG" "MON" "NIX" "NOT" "OFF" "OMS" "RAW"
"ROW" "SAP" "SET" "SGA" "SHG" "SID" "SQL" "SYS" "TMP" "UID" "USR" "VAR")

if /i "%1" == "-check" goto :check
if /i "%1" == "-execute" goto :execute
if /i "%1" == "-describe" goto :describe

:usage:
    echo usage: %0 "{ -check | -describe | -execute }"
    set /a EXIT=99
    goto :exit

:check
    set /a EXIT=0
    goto :exit

:describe
    echo SM_PI_NAME:%name%
    echo SM_PI_DESCRIPTION:%description%
    set /a EXIT=0
    goto :exit

:execute
    set /a EXIT=0

    rem SM_TARGET_SID must be set
    if "%SM_TARGET_SID%" == "" (
        set /a EXIT=4
        echo SM_TARGET_SID not set
        goto :exit
    )

    rem exactly three alphanumeric characters, with starting with a letter
    echo %SM_TARGET_SID% | findstr "\<[a-zA-Z][a-zA-Z0-9][a-zA-Z0-9]\>"
>nul
    if %ERRORLEVEL% == 1 (
        set /a EXIT=4
        echo SID is defined as a 3 digit value starting with a letter.
[%SM_TARGET_SID%] is not valid.
```

```
        goto :exit
    )

    rem not a SAP reserved SID
    echo %INVALID_SIDS% | findstr /i \"%SM_TARGET_SID%\" >nul
    if %ERRORLEVEL% == 0 (
        set /a EXIT=4
        echo SID [%SM_TARGET_SID%] is reserved by SAP
        goto :exit
    )

    goto :exit



:exit
    echo Command complete.
    exit /b %EXIT%
```

Aufgabenskripte werden erstellt

Sie können die Task-Skripte für vor- und Nachaufgaben sowie Richtlinien für Backup-, Restore- und Klonvorgänge erstellen, das Skript schreiben und die vordefinierten Umgebungsvariablen in Ihren Parametern einbeziehen. Sie können entweder ein neues Skript erstellen oder eines der SnapManager Beispielskripte ändern.

Bevor Sie mit dem Erstellen des Skripts beginnen, stellen Sie sicher, dass:

- Sie müssen das Skript auf eine bestimmte Weise strukturieren, damit es im Kontext einer SnapManager-Operation ausgeführt werden kann.
- Sie müssen das Skript auf der Grundlage der erwarteten Vorgänge, der verfügbaren Eingabeparameter und der Rückgabekonventionen erstellen.
- Sie müssen Protokollmeldungen einschließen und die Meldungen zu benutzerdefinierten Protokolldateien umleiten.

a. Erstellen Sie das Aufgabenskript, indem Sie das Beispielskript anpassen.

   Führen Sie Folgendes aus:

   i. Suchen Sie ein Beispielskript im folgenden Installationsverzeichnis:

      <default_install_Directory>\Plugins\Beispiele\Backup\create

   <default_install_Directory>\Plugins\Beispiele\Clone\create

   i. Öffnen Sie das Skript in Ihrem Skript-Editor.
   ii. Speichern Sie das Skript mit einem anderen Namen.

b. Ändern Sie die Funktionen, Variablen und Parameter nach Bedarf.

c. Das Skript in einem der folgenden Verzeichnisse speichern:

Skripts für Backup-Vorgänge

- <default_install_Directory>\Plugins\Backup\create\pre: Führt das Skript aus, bevor der Backup-Vorgang durchgeführt wird. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
- <default_install_Directory>\Plugins\Backup\create\post: Führt das Skript nach dem Backup-Vorgang aus. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
- <default_install_Directory>\Plugins\Backup\create\Policy: Führt das Skript immer aus, bevor der Backup-Vorgang erfolgt. SnapManager verwendet dieses Skript immer für alle Backups im Repository. **Betriebsskripte wiederherstellen**
- <default_install_Directory>\Plugins\restore\create\pre: Führt das Skript aus, bevor der Backup-Vorgang durchgeführt wird. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
- <default_install_Directory>\Plugins\restore\create\post: Führt das Skript nach dem Backup-Vorgang aus. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
- <default_install_Directory>\Plugins\restore\create\Policy: Führt das Skript immer aus, bevor der Backup-Vorgang erfolgt. SnapManager verwendet dieses Skript immer für alle Backups im Repository. **Clone Operation Scripts**
- <default_install_Directory>\Plugins\Clone\create\pre: Führt das Skript aus, bevor der Backup-Vorgang durchgeführt wird. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
- <default_install_Directory>\Plugins\Clone\create\post: Führt das Skript nach dem Backup-Vorgang aus. Verwenden Sie sie optional, wenn Sie die Backup-Erstellung angeben.
- <default_install_Directory>\Plugins\Clone\create\Policy: Führt das Skript immer aus, bevor der Backup-Vorgang erfolgt. SnapManager verwendet dieses Skript immer für alle Backups im Repository.

Speichern der Taskskripte

Sie müssen die Skript für Aufgaben vor, nach und nach der Aufgabe sowie die Richtlinien in einem bestimmten Verzeichnis auf dem Zielserver speichern, auf dem die Backups oder Klone erstellt werden. Für den Wiederherstellungsvorgang müssen die Skripte in das angegebene Verzeichnis auf dem Zielserver platziert werden, auf dem Sie das Backup wiederherstellen möchten.

1. Erstellen Sie Ihr Skript.
2. Speichern Sie das Skript an einem der folgenden Speicherorte:

Für den Backup-Vorgang

Verzeichnis	Beschreibung
<default_install_Directory >\Plugins\Backup\create\Policy	Die Richtlinieskripte werden vor den Backup-Vorgängen ausgeführt.
<default_install_Directory >\Plugins\Backup\create\pre	Die Vorverarbeitungsskripte führen die vor dem Backup aus.

<default_install_Directory >\Plugins\Backup\create\pre	Die nachverarbeitenden Skripte werden nach den Backup-Vorgängen ausgeführt.

Für den Wiederherstellungsvorgang

Verzeichnis	Beschreibung
<default_install_Directory >\Plugins\restore\create\Policy	Die Richtlinienskripte werden vor den Wiederherstellungsvorgängen ausgeführt.
<default_install_Directory >\Plugins\restore\create\pre	Die Vorverarbeitungsskripte werden vor der Wiederherstellung ausgeführt.
<default_install_Directory >\Plugins\restore\create\post	Die nachverarbeitenden Skripte werden nach den Wiederherstellungsvorgängen ausgeführt.

Für den Klonvorgang

Verzeichnis	Beschreibung
<default_install_Directory >\Plugins\Clone\create\Policy	Die Richtlinisskripte werden vor dem Klonbetrieb ausgeführt.
<default_install_Directory >\Plugins\Clone\create\pre	Die Vorverarbeitungsskripte werden vor den Klonvorgängen ausgeführt.
<default_install_Directory >\Plugins\Clone\create\post	Die nachverarbeitenden Skripte werden nach den Klonvorgängen ausgeführt.

Überprüfen der Installation von Plug-in-Skripten

SnapManager ermöglicht Ihnen die Installation und Verwendung benutzerdefinierter Skripte zur Ausführung verschiedener Vorgänge. SnapManager bietet Plug-ins für Backup-, Restore- und Klonvorgänge, mit denen Sie Ihre benutzerdefinierten Skripts vor und nach dem Backup-, Restore- und Klonvorgängen automatisieren können.

1. Geben Sie den folgenden Befehl ein:

   bbs Plugin Check -osccount os db Benutzername

   Wenn Sie die Option -osaccount nicht bereitstellen, erfolgt die Überprüfung der Plug-in-Script-Installation für den Administrator anstatt für einen bestimmten Benutzer.

   Der folgende Ausgang zeigt an, dass die Skripte „Policy 1“, „pre-Plugin1“ und „pre-Plugin2“ erfolgreich installiert wurden. Das Post-Plugin1-Skript ist jedoch nicht funktionsfähig.

```
            smo plugin check
Checking plugin directory structure ...
<installdir>\plugins\clone\policy
   OK: 'policy1' is executable

<installdir>\plugins\clone\pre
   OK: 'pre-plugin1' is executable and returned status 0
   OK: 'pre-plugin2' is executable and returned status 0

<installdir>\plugins\clone\post
   ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

Erstellen einer Aufgabenspezifikationsdatei

Sie können die Aufgabenspezifikationsdateien über eine grafische Benutzeroberfläche (GUI), eine Befehlszeilenschnittstelle (CLI) oder einen Texteditor erstellen. Diese Dateien werden für die vor- oder Nachverarbeitung während der Backup-, Restore- und Klonvorgänge verwendet.

1. Erstellen Sie eine Aufgabenspezifikationsdatei über GUI, CLI oder einen Texteditor.

   Sie können die Spezifikationsdatei basierend auf der Struktur der folgenden Beispielaufgabe Spezifikationsdatei erstellen:

```
<task-specification>
  <pre-tasks>
                <task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>name</name>
      <parameter>
          <name>name</name>
          <value>value</value>
       </parameter>
    </task>
  </post-tasks>
</task-specification>
```

2. Geben Sie den Skriptnamen ein.
3. Geben Sie den Parameternamen und den dem Parameter zugewiesenen Wert ein.
4. Speichern Sie die XML-Datei im richtigen Installationsverzeichnis.

Beispiel für Aufgabenspezifikation

```
  <task-specification>
    <pre-tasks>
      <task>
        <name>clone cleanup</name>
        <description>pre tasks for cleaning up the target
system</description>
        </task>
    </pre-tasks>
    <post-tasks>
      <task>
        <name>SystemCopy follow-up activities</name>
        <description>SystemCopy follow-up activities</description>
        <parameter>
          <name>SCHEMAOWNER</name>
          <value>SAMSR3</value>
        </parameter>
      </task>
      <task>
        <name>Oracle Users for OS based DB authentication</name>
        <description>Oracle Users for OS based DB
authentication</description>
        <parameter>
          <name>SCHEMAOWNER</name>
          <value>SAMSR3</value>
        </parameter>
        <parameter>
          <name>ORADBUSR_FILE</name>


<value\>E:\\mnt\\sam\\oradbusr.sql</value\>
        </parameter>
      </task>
      </post-tasks>
  </task-specification>
```

Durchführung von Backup-, Restore- und Klonvorgängen mithilfe von Prescript und Post-Scripts

Sie können Ihr eigenes Skript verwenden, während Sie Backup-, Restore- oder Klonvorgang initiieren. SnapManager zeigt eine Seite für die Aktivierung von Aufgaben im Assistenten zum Erstellen von Backups, zum Wiederherstellen oder Wiederherstellen oder zum Erstellen von Klonen an, wo Sie das Skript auswählen und Werte für alle Parameter angeben können, die vom Skript benötigt werden.

- Installieren Sie die Plug-in-Skripte am richtigen Speicherort für die SnapManager-Installation.

- Überprüfen Sie, ob die Plug-ins korrekt installiert sind, indem Sie den Befehl smsap Plugin Check verwenden.
- Stellen Sie sicher, dass Sie die BASH-Shell verwenden.

Führen Sie in der Befehlszeilenschnittstelle (CLI) den Skriptnamen auf, wählen Sie die Parameter aus und legen Sie die Werte fest.

1. Um zu überprüfen, ob Sie die BASH-Shell verwenden, geben Sie den folgenden Befehl an der Eingabeaufforderung:bash ein

   Alternativ können Sie an der Eingabeaufforderung den Befehl which-bash eingeben und die Befehlsausgabe als Startparameter des Skripts verwenden.

   Die BASH-Shell funktioniert einwandfrei, wenn kein Fehler auftritt.

2. Geben Sie für den Backup-Vorgang die Option -taskSpec ein und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation ein, um eine Vorverarbeitung oder eine Nachbearbeitung durchzuführen, die vor oder nach dem Backup durchgeführt werden soll: bbs Backup create -profile_Name {[-full {-online { -offline} [-contake {-hourly [-Daily { -Weekly} -unlimited}] [-confirm] [-dataces [-monthly-commentaces [-monthly-contaces] [-monthly-commoceptaces [-monthly}] [-monthly-commoceptaces [-monthly] [-monthly-loceptaces] [-] [-monthly-monthly] [-monthly-loceptaces [-] [-monthly-lo [-Backup-destpath1 [,[path2]] [-exclude-destpath1 [,path2]]] [-prunelogs {-all} -untilSCN - -Before {-dateyyy-MM-dd HH:mm:ss in -Monaten / -Wochen}} -prune-destprune_dest1,[prune]-Backups]

   Wenn der Backup-Plug-in-Vorgang fehlgeschlagen ist, werden nur der Plug-in-Name und der Rückgabecode angezeigt. Ihr Plug-in-Skript muss Protokollmeldungen enthalten und die Meldungen an die benutzerdefinierten Protokolldateien weiterleiten.

3. Geben Sie für die Wiederherstellung der Sicherung die Option -taskSpec ein und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation ein, um eine Vorverarbeitung oder eine Nachbearbeitung durchzuführen, die vor oder nach der Wiederherstellung stattfinden soll: bbs Backup Restore -profilprofile_Name {-Label<Label> -id<id>} {-files>←Tablespaces<Tablespaces> -complete} -controlfiles} [-recover {-alllogs -nologs -bis <bis><][-restorespec<restorespec>] [-verify taskup] [-dump] [-Force]

   Wenn der Vorgang zum Wiederherstellen des Plug-ins fehlgeschlagen ist, werden nur der Plug-in-Name und der Rückgabecode angezeigt. Ihr Plug-in-Skript muss Protokollmeldungen enthalten und die Meldungen an die benutzerdefinierten Protokolldateien weiterleiten.

4. Geben Sie für den Vorgang „Clone create“ die Option -taskSpec ein und geben Sie den absoluten Pfad der XML-Datei für die Aufgabenspezifikation ein, um eine Vorverarbeitung oder eine Nachbearbeitung durchzuführen, die vor oder nach dem Klonvorgang stattfinden soll: bbs Clone create -profilprofile_Name {-Backup-labelBackup_Name←Backup-id} Backup-id> -current←newsidneft_sid -clonespepfull_path_to_clonespepecfile [-Reserve<yes, no, erben>] [-Host<Host>] [-Label<Label>] [-comment { comment>]←bose taskundspecs tasecute]

   Wenn der Klon-Plug-in-Vorgang fehlgeschlagen ist, werden nur der Plug-in-Name und der Rückgabecode angezeigt. Ihr Plug-in-Skript muss Protokollmeldungen enthalten und die Meldungen an die benutzerdefinierten Protokolldateien weiterleiten.

Beispiel für die Erstellung eines Backups mithilfe der XML-Datei für die Aufgabenspezifikation

```
smo backup create -profile SALES1 -full -online -taskspec
sales1_taskspec.xml -force -verify
```

Der Name des Speichersystems und der dem Profil zugeordneten Zieldatenbank-Hostname werden aktualisiert

Mit SnapManager 3.3 oder höher können Sie den Host-Namen des Speichersystems oder die Speichersystemadresse und den dem SnapManager-Profil zugeordneten Host-Namen der Zieldatenbank aktualisieren.

Der Name des Speichersystems, der einem Profil zugeordnet ist, wird aktualisiert

Mit SnapManager 3.3 oder höher können der Hostname oder die IP-Adresse eines Speichersystems, das einem Profil zugeordnet ist, aktualisiert werden.

Sie müssen Folgendes sicherstellen:

- Das Profil verfügt über mindestens eine Sicherung.

  Wenn das Profil keine Sicherungskopie hat, ist es nicht erforderlich, den Namen des Speichersystems für dieses Profil zu aktualisieren.

- Für das Profil wird kein Vorgang ausgeführt.

Sie können den Namen des Storage-Systems oder die IP-Adresse über die SnapManager Befehlszeilenschnittstelle (CLI) aktualisieren. Beim Aktualisieren des Namens des Speichersystems werden die in der Repository-Datenbank gespeicherten Metadaten aktualisiert. Nachdem Sie den Namen des Storage-Systems umbenannt haben, können Sie alle SnapManager-Vorgänge wie zuvor ausführen.

Sie können den Namen des Storage-Systems nicht mit der SnapManager Graphical User Interface (GUI) ändern.

Sie müssen sicherstellen, dass Snapshot Kopien im neuen Storage-System verfügbar sind. SnapManager überprüft nicht, ob die Snapshot Kopien im Storage-System vorhanden sind.

Sie müssen jedoch Folgendes beachten, während Sie ein Rolling Upgrade und Rollback des Hosts durchführen, nachdem Sie den Namen des Speichersystems umbenannt haben:

- Wenn Sie nach der Umbenennung des Speichersystemnamens ein Rolling Upgrade des Hosts durchführen, müssen Sie das Profil mit dem neuen Speichersystemnamen aktualisieren.
- Wenn Sie den Host nach der Umbenennung des Storage-Systems wieder starten, müssen Sie sicherstellen, dass Sie den Namen des Storage-Systems zurück auf den früheren Namen des Storage-Systems ändern, damit Sie die Profile, Backups und Klone des früheren Storage-Systems zur Durchführung von SnapManager-Vorgängen verwenden können.
  a. Geben Sie den folgenden Befehl ein: smo Storage rename -profilprofile-oldnameold_Storage_Name -newnamenew_Storage_Name [quiet / -verbose]

Ihr Ziel ist	Dann…

Aktualisieren Sie den Namen des Speichersystems, der einem Profil zugeordnet ist	Geben Sie die Option -profile an.
Aktualisieren Sie den Namen des Speichersystems oder die IP-Adresse, die einem Profil zugeordnet ist	Geben Sie die folgenden Optionen und Variablen an: • -Oldnameold_Storage_Name ist der Hostname oder die IP-Adresse des Speichersystems. • -Newnamenew_Storage_Name ist der Hostname oder die IP-Adresse des Speichersystems.

Im folgenden Beispiel wird der aktualisierte Speichersystemname angezeigt:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Anzeigen einer Liste von Speichersystemen, die einem Profil zugeordnet sind

Sie können eine Liste der Speichersysteme anzeigen, die einem bestimmten Profil zugeordnet sind.

Die Liste zeigt die Namen des Speichersystems an, die dem jeweiligen Profil zugeordnet sind.

Wenn für das Profil keine Backups verfügbar sind, können Sie den dem Profil zugeordneten Namen des Speichersystems nicht anzeigen.

1. Um Informationen zu Storage-Systemen anzuzeigen, die mit einem bestimmten Profil in Verbindung stehen, geben Sie den folgenden Befehl ein: smo Storage list -profilprofile [-quiet - verbose]

Beispiel

```
smo storage list -profile mjubllian
```

```
Sample Output:
Storage Controllers
--------------------
STCO1110-RTP07OLD
```

Der Host-Name der Zieldatenbank, der einem Profil zugeordnet ist, wird aktualisiert

SnapManager (3.2 oder höher) für Oracle bietet die Möglichkeit, den Hostnamen der Zieldatenbank im SnapManager-Profil zu aktualisieren.

- Das Home-Verzeichnis des lokalen Benutzers muss die Zuordnung zu den Profilen und Repositorys kennen.
- Die Sitzungen der SnapManager Graphical User Interface (GUI) müssen geschlossen werden.

Sie können das Profil mit dem neuen Hostnamen aktualisieren, indem Sie nur die CLI verwenden.

Szenarien werden nicht unterstützt, wenn der Hostname der Zieldatenbank im Profil geändert werden soll

Die folgenden Szenarien werden beim Ändern des Hostnamen der Zieldatenbank im Profil nicht unterstützt:

- Ändern des Host-Namens der Zieldatenbank mithilfe der SnapManager-GUI
- Rollback der Repository-Datenbank nach Aktualisierung des Host-Namens der Zieldatenbank des Profils durchführen
- Aktualisieren mehrerer Profile für einen neuen Hostnamen der Zieldatenbank durch Ausführen eines einzigen Befehls
- Ändern des Host-Namens der Zieldatenbank, wenn ein SnapManager-Vorgang ausgeführt wird

> Nachdem Sie den Hostnamen der Zieldatenbank im Profil aktualisiert haben, wird nur der Hostname der Zieldatenbank geändert. Alle anderen Konfigurationsparameter, die im Profil festgelegt sind, werden beibehalten.

Nachdem Sie den Hostnamen der Zieldatenbank aktualisiert haben, können Sie das Backup nicht löschen oder unmounten, wenn der Klon oder das bereitgestellte Backup nicht auf dem neuen Host verfügbar ist. In solchen Szenarien führen die Ausführung der SnapManager Vorgänge vom neuen Host zu Ausfällen sowie zu veralteten Einträgen im früheren Host. Um SnapManager-Vorgänge durchzuführen, müssen Sie zum früheren Hostnamen mithilfe der Profilaktualisierung zurücksetzen.

1. Geben Sie folgenden Befehl ein: smo-Profil-Update -profileprofil [-profile-passwordprofile_password][-Database-dbnamedb_dbname-hostdb_Host [-siddb_sid] [-Login-usernamedb_username-adressnum{] [-{ commentail] [-{ commansion-comments2}}}] [-association-comments2] [-commented_adressem] [-commentary] [-commentation_adressem_adressum] [-commentary] [-commentermninct] [-commendbmninct] [-commendbmninct] [-ledbmninct] [-commendb] [-ledb] [-commendb] [-commendbmpromproмations2] [-commendb] [-commendbmations2] [-commendb] [-commendb] [-commendbmprom

   Weitere Optionen für diesen Befehl:

   [-Force] [-noprompt]

Ihr Ziel ist	Dann…
Ändern Sie den Hostnamen der Zieldatenbank	Geben Sie -hostNew_db_Host an

2. Geben Sie zum Anzeigen des Host-Namens der Zieldatenbank des Profils den folgenden Befehl ein: smo Profile show

Historie von SnapManager-Vorgängen aufrechterhalten

Mit SnapManager für Oracle können Sie den Verlauf der SnapManager Vorgänge, die mit einem einzelnen Profil oder mehreren Profilen verknüpft sind, beibehalten. Sie können

den Verlauf entweder über die SnapManager Befehlszeilenschnittstelle (CLI) oder über die grafische Benutzeroberfläche (GUI) aufrechterhalten. Sie können die Historie der Vorgänge als Bericht anzeigen und den Bericht zu Audit-Compliance-Zwecken verwenden.

Sie können den Verlauf der folgenden SnapManager Vorgänge beibehalten:

- Backup erstellen
- Backup verifizieren
- Backup Restore
- Klon erstellen

Die Verlaufsinformationen für die SnapManager Vorgänge werden basierend auf der Aufbewahrung beibehalten. Sie können für jeden der unterstützten SnapManager Vorgänge unterschiedliche Aufbewahrungsklassen konfigurieren.

Im Folgenden sind einige Aufbewahrungsklassen aufgeführt, die Sie zuweisen können:

- Anzahl Tage
- Anzahl Wochen
- Anzahl Monate
- Anzahl an Operationen

Basierend auf der Aufbewahrung bereinigt SnapManager die Historie automatisch. Außerdem können Sie die Historie der SnapManager-Vorgänge manuell löschen. Wenn Sie das Profil löschen oder zerstören, werden alle dem Profil zugeordneten Verlaufsdaten gelöscht.

Nach dem Rollback des Hosts können Sie die Verlaufsdaten nicht anzeigen oder mit dem Profil, das für die Verlaufswartung konfiguriert wurde, verbundene Vorgänge durchführen.

Konfigurieren des Verlaufs für den SnapManager-Vorgang

Mit SnapManager für Oracle können Sie den Verlauf des SnapManager-Betriebs über die Befehlszeilenschnittstelle oder Benutzeroberfläche von SnapManager aufrechterhalten. Sie können den Verlauf der SnapManager-Operation als Bericht anzeigen.

1. Um den Verlauf der SnapManager-Operation zu konfigurieren, geben Sie folgenden Befehl ein: smo history set -profile {-Name, profile_Name [profile_name1, profile_name2] -all-Repository-Login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname_portrepo_Port} -Operation {} {}-operationOperation_Name [unbose_restay_all_restay_restay_rejour]

```
        smo
history set -profile -name PROFILE1 -operation -operations backup -retain
-daily 6 -verbose
```

```
        smo
history set -profile -name PROFILE1 -operation -all -retain -weekly 3
-verbose
```

Anzeigen einer Liste des SnapManager-Betriebsverlaufs

Sie können den Verlauf eines bestimmten oder aller SnapManager Vorgänge basierend auf den Aufbewahrungseinstellungen als Bericht anzeigen.

1. Um eine Liste der SnapManager-Verlaufsvorgänge anzuzeigen, geben Sie den folgenden Befehl ein: smo-Verlaufsliste -profile {-Name, profile_Name [Profile_name1,profile_name2] -all-Repository-Login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname_Host-portrepo_Port} -Operation {}-operationsOperation_Name [bose_Name]

Anzeigen des detaillierten Verlaufs einer bestimmten Operation, die einem Profil zugeordnet ist

Sie können den detaillierten Verlauf einer bestimmten SnapManager Operation anzeigen, die einem Profil zugeordnet ist.

1. Um detaillierte Verlaufsinformationen über eine bestimmte SnapManager-Operation anzuzeigen, die einem Profil zugeordnet ist, geben Sie den folgenden Befehl ein: `smo history operation-show -profileprofile_name {-labellabel | -ididl} [-quiet | -verbose]`

Löschen des Verlaufs des SnapManager-Vorgangs

Sie können den Verlauf des SnapManager-Vorgangs löschen, wenn Sie keine Verlaufsdetails mehr benötigen.

1. Um den Verlauf der SnapManager-Operation zu löschen, geben Sie folgenden Befehl ein: smo-History purge -profile {-Name, profile_nameprofile_name1, profile_name2] All-Repository-Login [-passwordrepo_password] -usernamerepo_username-dbnamerepo_dbname_portrepo_Port} -Operation {}-namense1_Operation_Name [Operation_nece1]

Entfernen von Verlaufseinstellungen, die einem einzelnen Profil oder mehreren Profilen zugeordnet sind

Mit SnapManager können Sie die Verlaufseinstellungen eines SnapManager-Vorgangs entfernen. Mit diesem Vorgang werden alle Verlaufsdaten gelöscht, die mit einem einzelnen Profil oder mehreren Profilen verknüpft sind.

1. Um den Verlauf der SnapManager-Vorgänge zu entfernen, die mit einem einzelnen Profil oder mehreren Profilen verknüpft sind, geben Sie den folgenden Befehl ein: smo-history remove -profile {-Name, profile_Name [profile_name1, profile_name2] All-Repository-Login [-passwordrepo_password] -usernamerepo_usernamerepo_dbname-hostrepo_Host-portrepo_Port} -Operation {} -unbose_necen1

Anzeigen der Konfigurationsdetails des SnapManager-Verlaufs

Sie können die Verlaufseinstellungen für ein einzelnes Profil anzeigen.

Im SnapManager-Verlauf werden für jedes Profil die folgenden Informationen angezeigt:

- Name des Vorgangs
- Aufbewahrungsklasse
- Anzahl der Aufbewahrung
  a. Um Informationen über die Operation „SnapManager History“ für ein bestimmtes Profil anzuzeigen, geben Sie den folgenden Befehl ein: smo history show -profilprofile_Name

Befehlsreferenz für SnapManager für Oracle

Die SnapManager-Befehlsreferenz enthält die gültige Syntax, Optionen, Parameter und Argumente, die Sie zusammen mit Beispielen mit den Befehlen bereitstellen sollten.

Die folgenden Probleme gelten für die Verwendung von Befehlen:

- Bei Befehlen wird die Groß-/Kleinschreibung beachtet.
- SnapManager akzeptiert bis zu 200 Zeichen und Labels mit bis zu 80 Zeichen.
- Wenn die Shell auf Ihrem Host die Anzahl der Zeichen begrenzt, die in einer Befehlszeile angezeigt werden können, können Sie den Befehl cmdfile verwenden.
- Verwenden Sie keine Leerzeichen in Profilnamen oder Namen.
- Verwenden Sie in der Klonspezifikation keine Leerzeichen am Klonspeicherort.

SnapManager kann drei Meldungsebenen in der Konsole anzeigen:

- Fehlermeldungen
- Warnmeldungen
- Informationsmeldungen

Sie können festlegen, wie Meldungen angezeigt werden sollen. Wenn Sie nichts angeben, wird in SnapManager nur Fehlermeldungen und Warnmeldungen an der Konsole angezeigt. Verwenden Sie eine der folgenden Befehlszeilenoptionen, um die Menge der Ausgabe, die SnapManager in der Konsole angezeigt wird:

- -Quiet: Zeigt nur Fehlermeldungen an der Konsole an.
- -Verbose: Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Unabhängig vom Standardverhalten oder der Detailebene, die Sie für die Anzeige angeben, schreibt SnapManager immer alle Nachrichtentypen in die Protokolldateien.

Der Befehl smo_Server restart

Mit diesem Befehl wird der SnapManager-Hostserver neu gestartet und als root eingegeben.

Syntax

```
        smo_server restart
[-quiet | -verbose]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen auf der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen auf der Konsole angezeigt werden.

Beispielbefehl

Im folgenden Beispiel wird der Host-Server neu gestartet.

```
smo_server restart
```

Der Befehl smo_Server Start

Mit diesem Befehl wird der Host-Server gestartet, auf dem die SnapManager für Oracle-Software ausgeführt wird.

Syntax

```
        smo_server start
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen auf der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen auf der Konsole angezeigt werden.

Beispielbefehl

Das folgende Beispiel startet den Host-Server.

```
smo_server start
SMO-17100: SnapManager Server started on secure port 25204 with PID 11250
```

Der Status-Befehl smo_Server

Sie können den smo_Server Status Befehl ausführen, um den Status des SnapManager Host Servers anzuzeigen.

Syntax

```
        smo_server status
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen in der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen in der Konsole angezeigt werden.

Beispiel

Im folgenden Beispiel wird der Status des Host-Servers angezeigt:

```
smo_server status
SMO-17104: SnapManager Server version 3.3.1 is running on secure port
25204 with PID 11250
  and has 0 operations in progress.
```

Der Befehl smo_Server stop

Dieser Befehl stoppt den SnapManager-Hostserver und wird im Root eingegeben.

Syntax

```
        smo_server stop
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen auf der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen auf der Konsole angezeigt werden.

Beispielbefehl

Im folgenden Beispiel wird der Befehl smo_Server stop verwendet.

```
smo_server stop
```

Der Befehl smo Backup erstellen

Sie können den Befehl Backup create ausführen, um Datenbank-Backups auf einem oder mehreren Speichersystemen zu erstellen.

Syntax

Bevor Sie diesen Befehl ausführen, müssen Sie ein Datenbankprofil mithilfe des Befehls Profile create erstellen erstellen.

```
        smo backup create
-profile profile_name
{\[-full\{-auto \| -online \| -offline\}\[-retain \{-hourly \| -daily \|
-weekly \| -monthly \| -unlimited\} \[-verify\]  |
\[-data \[\[-files files \[files\]\] \|
\[-tablespaces tablespaces \[tablespaces\]\] \[-label label\] \{-auto \|
-online \| -offline\}
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\} \[-
verify\] |
\[-archivelogs \[-label label\]\] \[-comment comment\]}

\[-backup-dest path1 \[ , path2\]\]
\[-exclude-dest path1 \[ , path2\]\]
\[-prunelogs \{-all \| -until-scn until-scn \| -until-date yyyy-MM-
dd:HH:mm:ss\] \| -before \{-months \| -days \| -weeks \| -hours}}
-prune-dest prune_dest1,\[prune_dest2\]\]
\[-taskspec taskspec\]
\[-dump\]
-force
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die gesichert werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Auto Option**

  Wenn die Datenbank im Status „angehängt“ oder „Offline“ steht, führt SnapManager ein Offline-Backup durch. Wenn sich die Datenbank im offenen oder Online-Status befindet, führt SnapManager ein Online-Backup durch. Wenn Sie die Option -Force mit der Option -offline verwenden, erzwingt SnapManager ein Offline-Backup, selbst wenn die Datenbank derzeit online ist.

- **-Online-Option**

  Gibt ein Online-Datenbank-Backup an.

  - Wenn sich die lokale Instanz im Status beim Herunterfahren befindet und sich mindestens eine Instanz im offenen Status befindet, können Sie die Option -Force verwenden, um die lokale Instanz in den angehängten Status zu ändern.
  - Wenn sich keine Instanz im Status „Open“ befindet, können Sie die Option „-Force“ verwenden, um die lokale Instanz in den Status „Open“ zu ändern.

- **-Offline-Option**

  Gibt ein Offline-Backup an, während sich die Datenbank im Status Herunterfahren befindet. Wenn sich die Datenbank im offenen oder gemounteten Status befindet, schlägt das Backup fehl. Wenn die Option -Force verwendet wird, versucht SnapManager, den Datenbankstatus zu ändern, um die Datenbank für ein

Offline-Backup herunterzufahren.

- **-Volloption**

  Sicherung der gesamten Datenbank. Dazu gehören alle Daten, archivierte Log- und Kontrolldateien. Die archivierten Wiederherstellungsprotokolle und Kontrolldateien werden gesichert, unabhängig davon, welche Art von Backup Sie durchführen. Wenn Sie nur einen Teil der Datenbank sichern möchten, verwenden Sie die Option -files oder -Tablespaces.

- **-Datenoption**

  Gibt die Datendateien an.

- **-Dateiliste**

  Sichert nur die angegebenen Datendateien sowie die archivierten Protokoll- und Kontrolldateien. Trennen Sie die Liste der Dateinamen mit Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * -Tablespaces*

  Sicherung nur der angegebenen Datenbanktablespaces plus der archivierten Protokoll- und Kontrolldateien Trennen Sie die Namen der Tablespaces durch Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * Label*

  Gibt einen optionalen Namen für dieses Backup an. Dieser Name muss innerhalb des Profils eindeutig sein. Der Name kann Buchstaben, Zahlen, Unterstriche (_) und Bindestriche (-) enthalten. Es kann nicht mit einem Bindestrich beginnen. Wenn Sie keine Beschriftung angeben, erstellt SnapManager im Scope_type_date-Format eine Standardbeschriftung:

  - Der Umfang ist entweder F, um ein vollständiges Backup anzuzeigen, oder P, um auf ein teilweises Backup hinzuweisen.
  - Geben Sie C ein, um ein Offline-Backup (Cold) anzuzeigen, H für ein Online-Backup (Hot) oder Ein Für die automatische Sicherung, z. B. P_A_20081010060037IST, anzuzeigen.
  - Datum ist Jahr, Monat, Tag und Uhrzeit des Backups.

    SnapManager verwendet eine 24-Stunden-Zeit.

  Beispiel: Wenn Sie am 16. Januar 2007 um 5:45:16 Uhr eine vollständige Sicherung mit offline der Datenbank durchgeführt haben Eastern Standard Time, SnapManager würde die Bezeichnung F_C_20070116174516EST erstellen.

- **-comment-Zeichenfolge**

  Gibt einen optionalen Kommentar an, um dieses Backup zu beschreiben. Schließen Sie die Zeichenfolge in einzelne Anführungszeichen (').

  > Einige Schalen entfernen die Anführungszeichen. In diesem Fall müssen Sie das Anführungszeichen mit einem umgekehrten Schrägstrich (\) angeben. Möglicherweise müssen Sie Folgendes eingeben: `\' this is a comment\'`.

- **-Verify Option**

Überprüft, ob die Dateien im Backup nicht beschädigt sind, indem Sie das Oracle dbv-Dienstprogramm ausführen.

Wenn Sie die Option -verify angeben, wird der Backup-Vorgang erst abgeschlossen, wenn der Überprüfungvorgang abgeschlossen ist.

- **-Force Option**

  Erzwingt eine Statusänderung, wenn sich die Datenbank nicht im richtigen Zustand befindet. Beispielsweise kann SnapManager den Status der Datenbank von Online- in Offline-Modus ändern, basierend auf dem von Ihnen angegebenen Backup-Typ und dem Status, in dem sich die Datenbank befindet.

  - Wenn sich die lokale Instanz im Status beim Herunterfahren befindet und sich mindestens eine Instanz im offenen Status befindet, wird die lokale Instanz mit der Option -Force in den angehängten Status geändert.
  - Wenn sich keine Instanz im Status Open befindet, wird die lokale Instanz mithilfe der Option -Force in den Status Open geändert.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

- **-halten Sie { - stündlich - jeden Tag — monatlich - unbegrenzt}**

  Gibt an, ob das Backup stündlich, täglich, wöchentlich, monatlich oder unbegrenzt aufbewahrt werden soll. Wenn die Option -Retention nicht angegeben ist, orientiert sich die Retention class standardmäßig an der Option -hourly. Mit der Option -unlimited können Sie Backups für immer aufbewahren. Die Option -unlimited macht das Backup nicht zur Löschung durch die Aufbewahrungsrichtlinie.

- **-Archivprotokolle-Option**

  Erstellt Backup für Archivprotokolle

- **-Backup-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll an, die für die Sicherung des Archivprotokolls gesichert werden sollen.

- **-exclude-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll an, die vom Backup ausgeschlossen werden sollen.

- *-prunelogs {-all} -bis-scnbis-scn - bis-dateyyyyy-MM-dd:HH:mm:ss - vor {-Monaten

  Löscht die Archivprotokolldateien aus den Zielen des Archivprotokolls basierend auf den bei der Erstellung eines Backups bereitgestellten Optionen. Die Option -all löscht alle Archivprotokolldateien aus den Archivprotokollzielen. Mit der Option -bis-scn werden die Archivprotokolldateien bis zu einer angegebenen Systemänderungsnummer (SCN) gelöscht. Mit der Option -bis-date werden die Archivprotokolldateien bis zum angegebenen Zeitraum gelöscht. Die Option -before löscht die Archivprotokolldateien vor dem

angegebenen Zeitraum (Tage, Monate, Wochen, Stunden).

- **-prune-dest prune_dest1,prune_dest2**

  Löscht die Archivprotokolldateien aus den Archivprotokollzielen, während die Sicherung erstellt wird.

- **-taskSpec taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation an, die für die Vorverarbeitung oder Nachverarbeitung des Backup-Vorgangs verwendet werden kann. Der vollständige Pfad der XML-Datei sollte zur Verfügung gestellt werden, während die Option -taskSpec angegeben wird.

- **-dump-Option**

  Sammelt die Speicherauszugsdateien nach einem erfolgreichen oder fehlgeschlagenen Datenbanksicherungvorgang.

Beispielbefehl

Mit dem folgenden Befehl wird ein vollständiges Online Backup erstellt, ein Backup auf dem Sekundärspeicher erstellt und die Aufbewahrungsrichtlinie auf einen täglichen Routineaufgaben setzt:

```
smo backup create -profile SALES1 -full -online
-label full_backup_sales_May -profile SALESDB -force -retain -daily
Operation Id [8abc01ec0e79356d010e793581f70001] succeeded.
```

Verwandte Informationen

Datenbank-Backups werden erstellt

Der Befehl smo profile create

Der Befehl smo Backup delete

Sie können den Befehl zum Löschen von Backups ausführen, um Backups zu entfernen, die nicht automatisch entfernt werden, z. B. Backups, die zum Erstellen eines Klons oder einer fehlgeschlagenen Backups verwendet wurden. Sie können Backups, die unbegrenzt aufbewahrt werden, ohne die Aufbewahrungsklasse zu ändern.

Syntax

```
        smo backup delete
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Datenbank an, die mit dem Backup verknüpft ist, das Sie entfernen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Gibt das Backup mit der angegebenen GUID an. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Gibt das Backup mit der angegebenen Bezeichnung an. Geben Sie optional den Umfang des Backups als Datendatei oder Archivprotokoll an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-alle**

  Gibt alle Backups an. Verwenden Sie zum Löschen nur der angegebenen Backups die Option -id oder -Label.

- **-dump**

  Sammelt die Speicherauszugsdateien nach einem erfolgreichen oder fehlgeschlagenen Backup-Löschvorgang.

- **-Force**

  Erzwingt das Entfernen der Sicherung. SnapManager entfernt das Backup, selbst wenn es Probleme gibt, die mit dem Backup verbundenen Ressourcen freisetzen. Wenn das Backup beispielsweise mit dem Oracle Recovery Manager (RMAN) katalogisiert wurde, aber die RMAN-Datenbank nicht mehr existiert, einschließlich -Force löscht das Backup, obwohl es keine Verbindung mit RMAN herstellen kann.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Backup gelöscht:

```
smo backup delete -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Verwandte Informationen

Backups werden gelöscht

Der Befehl smo profile create

Der Befehl smoprofile Update

Der smo Backup kostenlose Befehl

Sie können den kostenlosen Befehl für die Sicherung ausführen, um die Snapshot-Kopien der Backups freizumachen, ohne die Backup-Metadaten aus dem Repository zu entfernen.

Syntax

```
        smo backup free
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid \| -all\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, das mit dem Backup verknüpft ist, das Sie freigeben möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Gibt die Ressourcen des Backups mit der angegebenen GUID an. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen. Schließen Sie die -verbose Option zum Anzeigen der Backup-IDs an.

- * Label*

  Gibt das Backup mit der angegebenen Bezeichnung an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

Gibt die Archivprotokolldateien an.

- **-alle**

  Gibt alle Backups an. Verwenden Sie zum Löschen der angegebenen Backups die Option -id oder -Label.

- **-Force**

  Erzwingt das Entfernen der Snapshot Kopien.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Das folgende Beispiel entlastet das Backup:

```
smo backup free -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Verwandte Informationen

So werden Backups entlastet

Der Befehl smo Backup list

Sie können den Befehl Backup list ausführen, um Informationen zu den Backups in einem Profil anzuzeigen, einschließlich Informationen zur Aufbewahrungsklasse und zum Sicherungsstatus.

Syntax

```
        smo backup list
-profile profile_name
-delimiter character
[-data | -archivelogs | -all]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie Backups auflisten möchten. Das Profil enthält die Kennung der Datenbank

und andere Datenbankinformationen.

- **-Trennzeichen**

  Zeigt jede Zeile in einer eigenen Zeile an. Die Attribute in der Zeile werden durch das angegebene Zeichen getrennt.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an. Schließen Sie die -verbose Option zum Anzeigen der Backup-IDs an.

Beispiel

Im folgenden Beispiel werden die Backups für DAS SALES1-Profil aufgeführt:

```
smo backup list -profile SALES1 -verbose
Start Date          Status  Scope  Mode    Primary  Label      Retention
Protection
------------------- ------- ------ ------- -------- -----      --------
----------
2007-08-10 14:12:31 SUCCESS FULL   ONLINE  EXISTS   backup2    HOURLY
NOT REQUESTED
2007-08-05 12:08:37 SUCCESS FULL   ONLINE  EXISTS   backup4    UNLIMITED
NOT REQUESTED
2007-08-04 22:03:09 SUCCESS FULL   ONLINE  EXISTS   backup6    UNLIMITED
NOT REQUESTED
```

Verwandte Informationen

Anzeigen einer Liste von Backups

Der Befehl smo Backup Mount

Sie können den Befehl Backup Mount ausführen, um ein Backup anzuhängen, um einen Wiederherstellungsvorgang mit einem externen Tool durchzuführen.

Syntax

```
        smo backup mount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
[-host  host]

\[-dump\]
[-quiet | -verbose]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, das mit dem Backup verknüpft ist, das Sie mounten möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Bindet das Backup mit der angegebenen GUID ein. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Bindet das Backup mit dem angegebenen Etikett an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- * Host*

  Gibt den Host an, auf dem das Backup gemountet werden soll.

- **-dump**

  Sammelt die Speicherauszugsdateien nach dem erfolgreichen oder fehlgeschlagenen Mount-Vorgang.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Sie müssen diesen Befehl nur verwenden, wenn Sie ein externes Tool wie Oracle Recovery Manager (RMAN) verwenden. SnapManager übernimmt automatisch das Mounten von Backups, wenn Sie den smom Backup Restore Befehl verwenden, um das Backup wiederherzustellen. Mit diesem Befehl wird eine Liste angezeigt, die die Pfade anzeigt, auf denen die Snapshot Kopien angehängt wurden. Diese Liste wird nur angezeigt, wenn die Option -verbose angegeben ist.

Beispiel

Das folgende Beispiel hängt den Backup ab:

```
smo backup mount -profile SALES1 -label full_backup_sales_May -verbose
[INFO ]: SMO-13051: Process PID=6852
[INFO ]: SMO-13036: Starting operation Backup Mount on host
hadley.domain.private
[INFO ]: SMO-13036: Starting operation Backup Mount on host
hadley.domain.private
[INFO ]: SMO-13046: Operation GUID 8abc01573883daf0013883daf5ac0001
starting on Profile FAS_P1
[INFO ]: SD-00025: Beginning to connect filesystem(s) [I:\] from snapshot
smo_fas_p1_fasdb_d_h_2_8abc0157388344bc01388344c2d50001_0.
[INFO ]: SD-00016: Discovering storage resources for
C:\SnapManager_auto_mounts\I-2012071400592328_0.
[INFO ]: SD-00017: Finished storage discovery for
C:\SnapManager_auto_mounts\I-2012071400592328_0
[INFO ]: SD-00026: Finished connecting filesystem(s) [I:\] from snapshot
smo_fas_p1_fasdb_d_h_2_8abc0157388344bc01388344c2d50001_0.
[INFO ]: SD-00025: Beginning to connect filesystem(s) [H:\] from snapshot
smo_fas_p1_fasdb_d_h_1_8abc0157388344bc01388344c2d50001_0.
[INFO ]: SD-00016: Discovering storage resources for
C:\SnapManager_auto_mounts\H-2012071400592312_0.
[INFO ]: SD-00017: Finished storage discovery for
C:\SnapManager_auto_mounts\H-2012071400592312_0.
[INFO ]: SD-00026: Finished connecting filesystem(s) [H:\] from snapshot
smo_fas_p1_fasdb_d_h_1_8abc0157388344bc01388344c2d50001_0.
[INFO ]: SMO-13048: Backup Mount Operation Status: SUCCESS
[INFO ]: SMO-13049: Elapsed Time: 0:19:05.620
```

Verwandte Informationen

Montage von Backups

Der Smo Backup Restore Befehl

Sie können den Befehl Backup Restore ausführen, um Backups einer Datenbank oder eines Teils einer Datenbank wiederherzustellen, und optional die Datenbankinformationen wiederherstellen.

Syntax

```
        smo backup restore
-profile profile_name
\[-label label \| -id id\]
\[-files files \[files...\] \|
-tablespaces tablespaces \[tablespaces...\]\] \|
-complete \| -controlfiles\]
\[-recover \{-alllogs \| -nologs \| -until until\} \[-using-backup-
controlfile\] \]
\[-restorespec restorespec \| \]\]
\[-preview\]

\[-recover-from-location path1 \[, path2\]\]
\[-taskspec taskspec\]
\[-dump\]
\[-force\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Datenbank an, die wiederhergestellt werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- * Name des Etiketts*

  Stellt das Backup mit dem angegebenen Etikett wieder her.

- **-id-Guid**

  Stellt die Sicherung mit der angegebenen GUID wieder her. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- **Wählen Sie alle oder bestimmte Dateien**

  Optional können Sie eine der folgenden Optionen verwenden:

  - -Complete: Stellt alle Dateien in der Sicherung wieder her.
  - -Tablespaceslist: Stellt nur die angegebenen Tablespaces aus dem Backup wieder her.

    Sie müssen Leerzeichen verwenden, um die Namen in der Liste zu trennen.

  - -Fileslist: Stellt nur die angegebenen Datendateien aus dem Backup wieder her.

    Sie müssen Leerzeichen verwenden, um die Namen in der Liste zu trennen. Wenn die Datenbank ausgeführt wird, stellt SnapManager sicher, dass der Tablespace, der die Dateien enthält, offline ist.

- **-controlfiles**

  Stellt die Kontrolldateien wieder her. SnapManager ermöglicht Ihnen, in einem einzigen Vorgang Kontrolldateien zusammen mit den Datendateien aus den Backups wiederherzustellen. Die Option -controlfiles ist unabhängig von anderen Parametern für den Wiederherstellungsumfang, wie z. B. -Complete, -Tablespaces und -Files.

- **-Erholung**

  Stellt die Datenbank nach der Wiederherstellung wieder her. Sie müssen auch den Punkt angeben, an dem SnapManager die Datenbank wiederherstellen soll, indem Sie eine der folgenden Optionen verwenden:

  - -Nologs: Stellt die Datenbank zum Zeitpunkt der Sicherung wieder her und wendet keine Logs an.

    Sie können diesen Parameter für Online- oder Offline-Backups verwenden.

  - -Alllogs: Stellt die Datenbank auf die letzte Transaktion oder Commit wieder her und wendet alle erforderlichen Protokolle an.
  - -Bis Datum: Stellt die Datenbank bis zum angegebenen Datum und der angegebenen Zeit wieder her.

    Sie müssen das Jahr-Monat-Datum verwenden: Stunde: Minute: Sekunde (yyyy-mm-dd:hh:mm:ss) Format. Verwenden Sie für Stunden je nach Datenbankeinstellung entweder das 12-Stunden- oder das 24-Stunden-Format.

  - -Bis scn: Rollt die Datendateien weiter, bis sie die angegebene Systemändernummer (SCN) erreicht.
  - -Using-Backup-controlfile: Stellt die Datenbank mit der Backup-Kontrolldatei wieder her.

- **-restaurespec**

  Ermöglicht Ihnen, die Daten in einem aktiven File-System wiederherzustellen und aus den angegebenen Daten wiederherzustellen, indem Sie jede Original-Snapshot-Kopie einem aktiven File-System zuweisen. Falls Sie keine Option angeben, werden die Daten aus den Snapshot Kopien im primären Storage von SnapManager wiederhergestellt. Sie können eine der folgenden Optionen angeben:

  - -Restorespec: Gibt die wiederherzustellenden Daten und das Wiederherstellungsformat an.

- * Vorschau*

  Zeigt die folgenden Informationen an:

  - Zur Wiederherstellung jeder Datei wird der Wiederherstellungsmechanismus (Wiederherstellung von Storage-seitigen Dateisystemen, Dateiwiederherstellung auf Storage-Seite oder Dateikopien auf Host-Seite) verwendet
  - Warum effizientere Mechanismen nicht zur Wiederherstellung jeder Datei verwendet wurden, wenn Sie die Option -verbose angeben Wenn Sie die Option -Preview verwenden, müssen Sie Folgendes wissen:
  - Die Option -Force hat keine Auswirkung auf den Befehl.
  - Die Option -wiederherstellen hat keine Auswirkung auf den Befehl. Um eine Vorschau des Wiederherstellungsvorgangs anzuzeigen, muss die Datenbank gemountet werden. Wenn Sie eine Vorschau eines Wiederherstellungsplans anzeigen möchten und die Datenbank derzeit nicht angehängt ist, mountet SnapManager die Datenbank. Wenn die Datenbank nicht angehängt werden kann, schlägt der Befehl fehl, und SnapManager gibt die Datenbank in ihren ursprünglichen Status zurück.

Die Option -Preview zeigt bis zu 20 Dateien an. Sie können die maximale Anzahl von Dateien konfigurieren, die in der Datei smo.config angezeigt werden sollen.

- **-Recovery-from-location**

  Gibt den externen Speicherort der Archivprotokolldateien an. SnapManager nimmt die Archivprotokolldateien vom externen Standort auf und verwendet diese für den Recovery-Prozess.

- **-taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation für die Vorverarbeitung oder Nachbearbeitung des Wiederherstellungsvorgangs an. Sie müssen den vollständigen Pfad der XML-Datei für die Aufgabenspezifikation angeben.

- **-dump**

  Gibt an, die Speicherauszugsdateien nach dem Wiederherstellungsvorgang zu sammeln.

- **-Force**

  Ändert ggf. den Datenbankstatus in einen niedrigeren Status als der aktuelle Status.

  Standardmäßig kann SnapManager den Datenbankstatus während eines Vorgangs in einen höheren Status ändern. Diese Option ist nicht erforderlich, damit SnapManager die Datenbank in einen höheren Status ändert.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an. Sie können diese Option verwenden, um zu sehen, warum effizientere Wiederherstellungsprozesse nicht verwendet werden konnten, um die Datei wiederherzustellen.

Beispiel

Im folgenden Beispiel wird eine Datenbank zusammen mit den Kontrolldateien wiederhergestellt:

```
smo backup restore -profile SALES1 -label full_backup_sales_May
-complete -controlfiles -force
```

Verwandte Informationen

Datenbank-Backups werden wiederhergestellt

Wiederherstellen von Backups von einem alternativen Speicherort

Erstellen von Wiederherstellungsspezifikationen

Der Befehl smo Backup show

Mit dem Befehl Backup show können Sie detaillierte Informationen zu einem Backup anzeigen, einschließlich Sicherungsstatus, Backup-Aufbewahrungsklasse und Backups im primären und sekundären Speicher.

Syntax

```
        smo backup show
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Backups angezeigt werden sollen. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- * Label*

  Gibt die Bezeichnung des Backups an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-id-id**

  Gibt die Backup-ID an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen der Konsole sowie Klon- und Verifizierungsdaten an.

Beispiel

Im folgenden Beispiel werden ausführliche Informationen zum Backup angezeigt:

```
smo backup show -profile SALES1 -label BTNFS -verbose
Backup id: 8abc013111a450480111a45066210001
Backup status: SUCCESS
Primary storage resources: EXISTS
Protection sate: NOT REQUESTED
Retention class: DAILY
Backup scope: FULL
Backup mode: OFFLINE
Mount status: NOT MOUNTED
Backup label: BTNFS
Backup comment:
RMAN Tag: SMO_BTNFS_1175283108815
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Verification status: OK
Backup Retention Policy: NORMAL
Backup database: hsdb1
Checkpoint: 2700620
Tablespace: SYSAUX
Datafile: E:\disks\data\sysaux01.dbf [ONLINE]
...
Control Files:
File: E:\disks\data\control03.ctl
...
Archive Logs:
File: E:\disks\data\archive_logs\2_131_626174106.dbf
...
Host: Host1
File: E:\disks\data\hsdb\SMOBakCtl_1175283005231_0
...
Volume: hs_data
Snapshot: SMO_HSDBR_hsdb1_F_C_1_
8abc013111a450480111a45066210001_0
File: E:\disks\data\hsdb\SMOBakCtl_1175283005231_0
...
```

Verwandte Informationen

Anzeigen von Backup-Details

Der Befehl smo Backup unmount

Sie können den Befehl Backup unmount ausführen, um die Bereitstellung eines Backups zu aufheben.

Syntax

```
        smo backup unmount
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id id\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das die Bereitstellung eines Backups aufgehoben werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-id**

  Hängt das Backup mit der angegebenen GUID ab. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Hängt das Backup mit dem angegebenen Etikett ab.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-dump**

  Sammelt die Speicherauszugsdateien nach einem erfolgreichen oder fehlgeschlagenen Aushängevorgang.

- **-Force**

  Hängt das Backup ab, selbst wenn beim Freigeben der mit dem Backup verbundenen Ressourcen Probleme auftreten. SnapManager versucht, die Bereitstellung des Backups rückgängig zu machen und die zugehörigen Ressourcen zu bereinigen. Das Protokoll zeigt den Vorgang zum Aufheben der Bereitstellung als erfolgreich an. Bei Fehlern im Protokoll müssen Sie jedoch möglicherweise Ressourcen manuell bereinigen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im Folgenden finden Sie ein Beispiel für einen unmontierten Vorgang:

```
# smo backup unmount -label test -profile SALES1 -verbose
```

```
[INFO ]: SMO-13051: Process PID=9788
[INFO ]: SMO-13036: Starting operation Backup Unmount on host
hadley.domain.private
[INFO ]: SMO-13036: Starting operation Backup Unmount on host
hadley.domain.private
[INFO ]: SMO-13046: Operation GUID 8abc015738849a3d0138849a43900001
starting on Profile FAS_P1
[INFO ]: SD-00031: Beginning to disconnect filesystem(s)
[C:\SnapManager_auto_mounts\H-2012071400592312_0,
C:\SnapManager_auto_mounts\I-2012071400592328_0].
[INFO ]: SD-00032: Finished disconnecting filesystem(s)
[C:\SnapManager_auto_mounts\H-2012071400592312_0,
C:\SnapManager_auto_mounts\I-2012071400592328_0].
[INFO ]: SMO-13048: Backup Unmount Operation Status: SUCCESS
[INFO ]: SMO-13049: Elapsed Time: 0:07:26.754
```

Verwandte Informationen

UnMounten von Backups

Der SMO-Befehl zum Aktualisieren der Datensicherung

Sie können den Befehl Backup Update ausführen, um die Backup-Aufbewahrungsrichtlinie zu aktualisieren.

Syntax

```
        smo backup update
-profile profile_name
[-label label \[-data \| -archivelogs\] \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-comment comment_text\]
[-quiet | -verbose]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Backups aktualisiert werden sollen. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Überprüft die Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- * Label*

  Gibt das Backup-Label und den Umfang des Backups als Datendatei oder Archivprotokoll an.

- **-Daten**

  Gibt die Datendateien an.

- **-Archivprotokolle**

  Gibt die Archivprotokolldateien an.

- **-comment comment comment_Text**

  Geben Sie Text (bis zu 200 Zeichen) zum Backup-Update ein. Sie können Leerzeichen einschließen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

- **-halten Sie {-stündlich / -täglich / -monatlich / -unbegrenzt}**

  Gibt an, ob das Backup stündlich, täglich, wöchentlich, monatlich oder unbegrenzt aufbewahrt werden soll. Wenn -Retention nicht angegeben ist, wird die Aufbewahrungsklasse standardmäßig auf -hourly gesetzt. Mit der Option -unlimited können Sie Backups für immer aufbewahren. Die Option -unlimited macht das Backup nicht zum Löschen.

Beispiel

Im folgenden Beispiel wird das Backup aktualisiert, damit die Aufbewahrungsrichtlinie auf unbegrenzt gesetzt wird:

```
smo backup update -profile SALES1 -label full_backup_sales_May
-retain -unlimited -comment save_forever_monthly_backup
```

Verwandte Informationen

Ändern der Richtlinie zur Aufbewahrung von Backups

Dauerhaft Aufbewahrung von Backups

Freistellen oder Löschen von Backups ohne Rücknahmerichtlinien

Der Befehl smo Backup verify

Sie können den Befehl Backup Verify ausführen, um festzustellen, ob sich das Backup in einem gültigen Format für Oracle befindet.

Syntax

```
        smo backup verify
-profile profile_name
[-label backup_name \| \[-id guid\]
\[-retain \{-hourly \| -daily \| -weekly \| -monthly \| -unlimited\}\]
\[-force\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie ein Backup überprüfen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Überprüft die Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list verwenden, um die GUID für jedes Backup anzuzeigen.

- **-Label Label Label_Name**

  Überprüfung der Sicherung mit der angegebenen Bezeichnung.

- **-dump**

  Sammelt die Speicherauszugsdateien nach dem erfolgreichen oder fehlgeschlagenen Backup-Überprüfungvorgang.

- **-Force**

  Erzwingt die Datenbank in den erforderlichen Zustand, um den Verifizierungsvorgang durchzuführen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen

angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Das folgende Beispiel zeigt die Überprüfung des Backups:

```
smo backup verify -profile SALES1 -label full_backup_sales_May -quiet
```

```
DBVERIFY - Verification starting : FILE = C:\SnapManager_auto_mounts\H-
2012071400592312_0\smo\datafile\data
```

Verwandte Informationen

Datenbank-Backups werden überprüft

Der Befehl Smo Clone create

Sie können den Befehl Clone create ausführen, um einen Klon einer gesicherten Datenbank zu erstellen. Sie können ein Backup aus primärem oder sekundärem Storage klonen.

Syntax

```
        smo clone create
-profile profile_name
[-backup-id backup_guid \| -backup-label backup_label_name \| -current\]
-newsid new_sid
\[-host target_host\]
[-label clone_label]
\[-comment string\]
-clonespec full_path_to_clonespec_file
]
\[-syspassword syspassword\]
\[-reserve \{yes \| no \| inherit\}\]

\[-no-resetlogs \| -recover-from-location path1 \[, path2\]\]\[-taskspec
taskspec\]
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profilname**

  Gibt die Datenbank an, die geklont werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Backup-id Guid**

  Klont die Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Sie können den Befehl smo Backup list-verbose verwenden, um die GUID für jedes Backup anzuzeigen.

- **-Backup-Label Backup_Label_Name**

  Gibt an, dass das Backup mit dem angegebenen Namen geklont wird.

- **-Strom**

  Gibt an, dass Backup und Klon im aktuellen Status der Datenbank erstellt werden.

  Wenn sich die Datenbank im Noarchivlog Modus befindet, wird SnapManager ein offline Backup erstellen.

- **-newsid New_sid**

  Gibt eine neue, eindeutige Oracle-Systemkennung für die geklonte Datenbank an. Der Wert für die Systemkennung darf maximal acht Zeichen lang sein. Oracle erlaubt nicht, zwei Datenbanken mit derselben Systemkennung auf demselben Host gleichzeitig auszuführen.

- **-Host target_Host**

  Gibt den Host an, auf dem der Klon erstellt werden soll.

- **-Label Clone_Label**

  Gibt eine Bezeichnung für den Klon an.

- **-comment-Zeichenfolge**

  Gibt einen optionalen Kommentar an, um diesen Klon zu beschreiben. Sie müssen den String in einzelne Anführungszeichen einschließen.

  Einige Shells löschen die Anführungszeichen. Wenn das für Ihre Shell gilt, müssen Sie dem Angebot mit einem umgekehrten Schrägstrich (\) entkommen. Beispiel: \' Dies ist ein Kommentar\'

- **-clonespec full_path_to_clonespec_file**

  Gibt den Pfad zur XML-Datei für die Klonspezifikation an. Dies kann ein relativer oder ein absoluter Pfadname sein.

- **-syspassword-syspassword**

  Gibt das Kennwort für den Benutzer mit Systemprivilegierten an.

Sie müssen das Passwort für den Benutzer mit Systemberechtigungen angeben, wenn die angegebenen Datenbankanmeldeinformationen nicht für den Benutzer mit Systemprivilegierten identisch sind.

- **-Reserve**

  Wenn Sie die Option -Reserve auf ja einstellen, wird sichergestellt, dass die Speicherplatzreserve für die neuen Klon-Volumes aktiviert ist. Wenn die Option -Reserve auf Nein eingestellt wird, wird sichergestellt, dass die Speicherplatzreserve für die neuen Klon-Volumes deaktiviert ist. Durch Festlegen der Option -Reserve wird sichergestellt, dass der neue Klon die Eigenschaften der Platzreservierung der übergeordneten Snapshot Kopie übernimmt. Die Standardeinstellung ist Nein

  In der folgenden Tabelle werden die Klonmethoden und ihre Auswirkung auf den Vorgang zum Erstellen von Klonen und seine Option -Reserve beschrieben. Eine LUN kann mit beiden Methoden geklont werden.

Klonmethode	Beschreibung	Ergebnis
`LUN cloning`	`A new clone LUN is created within the same volume.`	`When the -reserve option for a LUN is set to yes, space is reserved for the full LUN size within the volume.`
`Volume cloning`	`A new FlexClone is created, and the clone LUN exists within the new clone volume. Uses the FlexClone technology.`	`When the -reserve option for a volume is set to yes, space is reserved for the full volume size within the aggregate.` +

- **-no-resetlogs**

  Gibt an, die Wiederherstellung der Datenbank zu überspringen, das DBNEWID Dienstprogramm auszuführen und nicht die Datenbank mit den Resetlogs während der Erstellung des Klons zu öffnen.

- **-Recovery-from-location**

  Gibt den externen Speicherort für das Archivprotokoll an, an dem SnapManager die Archivprotokolldateien vom externen Speicherort übernimmt und zum Klonen verwendet.

- **-taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation für die Vorverarbeitung oder Nachverarbeitung des

Klonvorgangs an. Sie müssen den vollständigen Pfad der XML-Datei für die Aufgabenspezifikation angeben.

- **-dump**

  Gibt an, die Dump-Dateien nach dem Erstellungsvorgang des Klons zu sammeln.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Backup mit einer Klonspezifikation geklont, die für diesen Klon erstellt wird:

```
smo clone create -profile SALES1 -backup-label full_backup_sales_May
-newsid
CLONE -label sales1_clone -clonespec E:\\spec\\clonespec.xml
```

```
Operation Id [8abc01ec0e794e3f010e794e6e9b0001] succeeded.
```

Verwandte Informationen

Erstellen von Klonspezifikationen

Klonen von Datenbanken aus Backups

Der Befehl smo Clone delete

Sie können den Befehl „Klon löschen“ ausführen, um einen Klon zu löschen. Sie können einen Klon nicht löschen, wenn der Klon für einen Vorgang verwendet wird.

Syntax

```
        smo clone delete
-profile profile_name
\[-id guid \| -label clone_name\]
[-login
\[-username db_username -password db_password -port db_port\]
 ]
\[-syspassword syspassword\]
-force
\[-dump\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das den zu löschenden Klon enthält. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Force**

  Löscht den Klon, auch wenn dem Klon Ressourcen zugeordnet sind.

- **-id-Guid**

  Gibt die GUID für den zu löschenden Klon an. Die GUID wird von SnapManager beim Erstellen eines Klons generiert. Sie können den Befehl smo Clone list verwenden, um die GUID für jeden Klon anzuzeigen.

- * Name des Etiketts*

  Gibt die Bezeichnung für den zu löschenden Klon an.

- **-syspassword-syspassword**

  Gibt das Kennwort für den Benutzer mit Systemprivilegierten an.

  > Sie müssen das Passwort für den Benutzer mit Systemberechtigungen angeben, wenn die angegebenen Datenbankanmeldeinformationen nicht für den Benutzer mit Systemprivilegierten identisch sind.

- **-Login**

  Ermöglicht die Eingabe der Anmeldedaten für die Datenbank.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist.

- **-Port db_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, die das Profil beschreibt.

- **-dump**

  Gibt an, die Speicherauszugsdateien nach dem Löschen des Klons zu sammeln.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird der Klon gelöscht:

```
smo clone delete -profile SALES1 -label SALES_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Der Befehl smo Clone list

Dieser Befehl listet die Klone der Datenbank für ein bestimmtes Profil auf.

Syntax

```
        smo clone list
-profile profile_name
-delimiter character
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Liste der mit dem Profil verknüpften Klone an. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Trennzeichen**

  Wenn dieser Parameter angegeben wird, führt der Befehl die Attribute in jeder Zeile durch das angegebene Zeichen getrennt auf.

- **-ruhig**

Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden die Datenbankklone im SALES1-Profil aufgeführt.

```
smo clone list -profile SALES1 -verbose
```

```
ID Status SID Host Label Comment
-------- ------- ----- ------- ---------- -------
8ab...01 SUCCESS hsdbc server1 back1clone test comment
```

Verwandte Informationen

Anzeigen einer Liste von Klonen

Der Befehl smo Clone show

Sie können den Befehl Clone show ausführen, um Informationen über die Datenbankklone für das angegebene Profil anzuzeigen.

Syntax

```
        smo clone show
-profile profile_name
\[-id  guid \| -label clone_name\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt die Liste der mit dem Profil verknüpften Klone an. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-Guid**

  Zeigt Informationen über den Klon mit der angegebenen GUID an. Die GUID wird von SnapManager beim Erstellen eines Klons generiert. Sie können den Befehl „smo Clone show“ verwenden, um die GUID für jeden Klon anzuzeigen.

- **-Label Label Label_Name**

Zeigt Informationen über den Klon mit der angegebenen Bezeichnung an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel werden Informationen über den Klon angezeigt:

```
smo clone show -profile SALES1 -label full_backup_sales_May -verbose
```

Die folgende Ausgabe zeigt Informationen zu einem Backup-Klon des primären Storage:

```
Clone id: 8abc013111b916e30111b916ffb40001
Clone status: SUCCESS
Clone SID: hsdbc
Clone label: hsdbc
Clone comment: null
Clone start time: 2007-04-03 16:15:50
Clone end time: 2007-04-03 16:18:17
Clone host: Host1
Filesystem: E:\ssys1\data_clone\
File: E:\ssys1\data_clone\hsdb\sysaux01.dbf
File: E:\ssys1\data_clone\hsdb\undotbs01.dbf
File: E:\ssys1\data_clone\hsdb\users01.dbf
File: E:\ssys1\data_clone\hsdb\system01.dbf
File: E:\ssys1\data_clone\hsdb\undotbs02.dbf
Backup id: 8abc013111a450480111a45066210001
Backup label: full_backup_sales_May
Backup SID: hsdb1
Backup comment:
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Backup host: server1
```

Verwandte Informationen

Anzeigen detaillierter Kloninformationen

Der Befehl smo Clone template

Mit diesem Befehl können Sie eine Vorlage für die Klonspezifikation erstellen.

Syntax

```
        smo clone template
-profile name
\[-backup-id guid  \| -backup-label backup_name\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profilname**

  Gibt die Datenbank an, für die Sie eine Klonspezifikation von erstellen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Backup-id Guid**

  Erstellt eine Klonspezifikation aus der Sicherung mit der angegebenen GUID. Die GUID wird von SnapManager beim Erstellen eines Backups generiert. Verwenden Sie den Befehl smo Backup list, um die GUID für jedes Backup anzuzeigen.

- **-Backup-Label Backup_Label_Name**

  Erstellt eine Klonspezifikation aus der Sicherung mit dem angegebenen Backup-Label.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel wird aus dem Backup eine Klon-Spezifikations-Vorlage mit dem Label full_Backup_Sales_May erstellt. Sobald der Befehl smo Clone Template abgeschlossen ist, ist die Klon-Spezifikations-Vorlage abgeschlossen.

```
smo clone template -profile SALES1 -backup-label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

Verwandte Informationen

Erstellen von Klonspezifikationen

Der Befehl smo Clone Update

Mit diesem Befehl werden Informationen zum Klon aktualisiert. Sie können den Kommentar aktualisieren.

Syntax

```
        smo clone update
-profile profile_name
\[-label label \| -id id\]
-comment  commment_text
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das den zu aktualisierenden Klon enthält. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-id-id**

  Gibt die ID für den Klon an. Die ID wird von SnapManager beim Erstellen eines Klons generiert. Verwenden Sie den Befehl smo Clone list, um die ID für jeden Klon anzuzeigen.

- * Label*

  Gibt die Bezeichnung für den Klon an.

- **-Kommentar**

  Zeigt den Kommentar an, der bei der Klonerstellung eingegeben wurde. Dies ist ein optionaler Parameter.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel wird der Klonkommentar aktualisiert.

```
smo clone update -profile anson.pcrac5
-label clone_pcrac51_20080820141624EDT -comment See updated clone
```

Der Befehl Smo Clone Trennen

Nach dem Aufteilen eines geklonten Volumes aus seinem übergeordneten Volume in Data ONTAP können Sie den Befehl „Clone Trennen“ (Abtrennen) von SnapManager ausführen und SnapManager darauf informieren, dass es sich bei dem Volume nicht mehr um einen Klon handelt.

Syntax

smo Clone Trennen -profile_Name -Label Clone_Label

Parameter

- **-profile Profile_Name**

  Gibt den Profilnamen an, aus dem der Klon erstellt wird.

- **-Label Clone_Label**

  Gibt den Namen an, der vom Klonvorgang generiert wurde.

Beispiel

Mit dem folgenden Befehl wird der Klon enttrennt:

```
smo clone detach -profile SALES1 -label sales1_clone
```

Der Befehl smo cmdfile

Sie können den Befehl cmdfile verwenden, um jeden beliebigen Befehl auszuführen, wenn die Shell auf Ihrem Host die Anzahl der Zeichen begrenzt, die in einer Befehlszeile angezeigt werden können.

Syntax

```
        smo cmdfile
-file file_name
\[-quiet \| -verbose\]
```

Sie können den Befehl in eine Textdatei einfügen und den Befehl smo cmdfile verwenden, um den Befehl auszuführen. Sie können nur einen Befehl in einer Textdatei hinzufügen. Sie dürfen smo nicht in die Befehlssyntax einschließen.

Der Befehl smo cmdfile ersetzt den Befehl smo pfile. Die smo cmdfile ist nicht mit dem Befehl smo pfile kompatibel.

Parameter

- **-file file_Name**

  Gibt den Pfad zur Textdatei an, die den Befehl enthält, den Sie ausführen möchten.

- **-ruhig**

  Gibt an, dass nur Fehlermeldungen in der Konsole angezeigt werden. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Gibt an, dass Fehler-, Warn- und Informationsmeldungen in der Konsole angezeigt werden.

Der Befehl smo Credential Clear

Mit diesem Befehl wird der Cache der Benutzeranmeldeinformationen für alle gesicherten Ressourcen gelöscht.

Syntax

```
        smo credential clear
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

In diesem Beispiel werden alle Anmeldeinformationen für den Benutzer gelöscht, der den Befehl ausführt.

```
smo credential clear -verbose
```

```
SMO-20024 [INFO ]: Cleared credentials for user "user1".
```

Verwandte Informationen

Löschen von Benutzeranmeldeinformationen für alle Hosts, Repositorys und Profile

Der Befehl zum Löschen von Smo-Anmeldeinformationen

Mit diesem Befehl werden die Benutzeranmeldeinformationen für eine bestimmte gesicherte Ressource gelöscht.

Syntax

```
        smo credential delete
\[-host -name host_name
-username username\] \|
[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port\] \|
\[-profile
-name profile_name\]
[-quiet | -verbose]
```

Parameter

- **-Host-Hostname**

  Gibt den Namen des Host-Servers an, auf dem SnapManager ausgeführt wird.

  Der Parameter -Host enthält die folgenden Optionen:

  - -Name Host_Name: Gibt den Namen des Hosts an, für den Sie das Passwort löschen möchten.
  - -Username user_Name: Gibt den Benutzernamen auf dem Host an.
- **-Repository -dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

  Der Parameter -Repository enthält die folgenden Optionen:

  - -Dbnamerepo_Service_Name: Gibt den Namen der Datenbank an, die das Profil speichert. Verwenden Sie entweder den globalen Namen oder den SID.
  - -Host repo_Host: Gibt den Namen oder die IP-Adresse des Hostservers an, auf dem die Repository-Datenbank ausgeführt wird.
  - -Login-username repo_username: Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.
  - -Port repo_Port: Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-profile -Name profile_Name**

  Gibt das Profil an, mit dem die Datenbank verknüpft ist.

  Der Parameter -profile enthält die folgende Option:

  - -Name profilname: Gibt den Namen des Profils an, für das Sie das Passwort löschen werden.
- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.
- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

In diesem Beispiel werden die Anmeldeinformationen des Profils gelöscht.

```
smo credential delete -profile -name user1 -verbose
```

```
SMO-20022 [INFO ]: Deleted credentials and repository mapping
 for profile "user1" in user credentials for "user1".
```

In diesem Beispiel werden die Anmeldeinformationen des Repositorys gelöscht.

```
smo credential delete -repository -dbname SMOREPO -host Host2
-login -username user1 -port 1521
```

```
SMO-20023 [INFO ]: Deleted repository credentials for
"user1@SMOREPO/wasp:1521"
and associated profile mappings in user credentials for "user1".
```

In diesem Beispiel werden die Anmeldeinformationen des Hosts gelöscht.

```
smo credential delete -host -name Host2
```

```
SMO-20033 [INFO ]: Deleted host credentials for "Host2" in user
credentials for "user1".
```

Verwandte Informationen

Löschen von Anmeldeinformationen für einzelne Ressourcen

Der Befehl smo Anmeldeinformationsliste

Dieser Befehl listet alle Anmeldedaten eines Benutzers auf.

Syntax

```
        smo credential list
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

In diesem Beispiel werden alle Anmeldeinformationen für den Benutzer angezeigt, der den Befehl ausführt.

```
smo credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMOREPO/hotspur:1521
Host2_test_user@SMOREPO/hotspur:1521
user1_1@SMOREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMOREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMOREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMOREPO/hotspur:1521) [PASSWORD NOT SET]
Hosts:
Host2
Host5
Host4
Host1
```

Verwandte Informationen

Anzeigen von Benutzeranmeldeinformationen

Der Befehl Smo Credential Set

Mit diesem Befehl können Sie die Anmeldeinformationen für Benutzer festlegen, die auf sichere Ressourcen wie Hosts, Repositorys und Datenbankprofile zugreifen können. Das Host-Passwort ist das Passwort des Benutzers auf dem Host, auf dem SnapManager ausgeführt wird. Das Repository-Kennwort ist das Kennwort des Oracle-Benutzers, der das SnapManager-Repository-Schema enthält. Das Profilkennwort ist ein Passwort, das von der Person, die das Profil erstellt, gebildet wird. Wenn bei den Host- und Repository-Optionen die Option optional -password nicht enthalten ist, werden Sie aufgefordert, ein Kennwort des in den Befehlsargumenten angegebenen Typs einzugeben.

Syntax

```
        smo credential set
\[-host
-name host_name
-username username\]
\[-password password\] \] \|
\[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username\] \[-password repo_password\] \]
-port repo_port \|
\[-profile
-name profile_name\]
\[-password password\] \]
\[-quiet \| -verbose\]
```

Parameter

- **-Host-Hostname**

  Gibt den Namen oder die IP-Adresse des Hostservers an, auf dem SnapManager ausgeführt wird.

  Der Parameter -Host enthält die folgenden Optionen:

  - -Name Host_Name: Gibt den Namen des Hosts an, für den Sie das Passwort festlegen möchten.
  - -Username user_Name: Gibt den Benutzernamen auf dem Host an.
  - -Password password: Gibt das Passwort des Benutzers auf dem Host an.

- **-Repository -dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

  Der Parameter -Repository enthält die folgenden Optionen:

  - -Dbnamerepo_Service_Name: Gibt den Namen der Datenbank an, die das Profil speichert. Verwenden

Sie entweder den globalen Namen oder den SID.

- -Host repo_Host: Gibt den Namen oder die IP-Adresse des Hostservers an, auf dem die Repository-Datenbank ausgeführt wird.
- -Login-username repo_username: Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.
- -Password password: Gibt das Kennwort an, das für den Zugriff auf die Datenbank, die das Repository speichert, erforderlich ist.
- -Port repo_Port: Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-profile -Name profile_Name**

  Gibt das Profil an, mit dem die Datenbank verknüpft ist.

  Der Parameter -profile enthält die folgende Option:

  - -Name profilname: Gibt den Namen des Profils an, für das Sie das Passwort festlegen.
  - -Password password: Gibt das Passwort an, das für den Zugriff auf das Profil erforderlich ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl zum Festlegen von Repository-Anmeldedaten

Im folgenden Beispiel werden Anmeldeinformationen für ein Repository festgelegt.

```
smo credential set -repository -dbname SMOREPO -host hotspur -port 1521
-login -username chris
Password for chris@hotspur:1521/SMOREPO : ********
Confirm password for chris@hotspur:1521/SMOREPO : ********
```

```
SMO-12345 [INFO ]: Updating credential cache for OS user "admin1"
SMO-12345 [INFO ]: Set repository credential for user "user1" on
repo1@Host2.
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

Beispiel-Befehl zum Festlegen von Host-Anmeldedaten

Da eine Hostanmeldeinformationen eine tatsächliche Betriebssystemanmeldeinformationen darstellen, muss sie zusätzlich zum Passwort den Benutzernamen enthalten.

```
smo credential set -host -name bismarck -username avida
Password for avida@bismarck : ********
Confirm password for avida@bismarck : ********
```

Verwandte Informationen

Wie SnapManager die Sicherheit gewährleistet

Der Befehl smo history list

Mit diesem Befehl können Sie eine Liste der Verlaufsdetails für den SnapManager-Vorgang anzeigen.

Syntax

```
        smo history list
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank

ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

  Gibt den SnapManager-Vorgang an, für den Sie den Verlauf konfigurieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history list -profile -name PROFILE1 -operation -operations
backup -verbose
```

Der Befehl smo history Operation-show

Mit diesem Befehl können Sie den Verlauf eines bestimmten SnapManager-Vorgangs, der einem Profil zugeordnet ist, anzeigen.

Syntax

```
        smo history operation-show
-profile profile
\{-label label \| -id id\}
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- * Label-Label. -idid*

  Gibt die SnapManager-Vorgangs-ID oder -Bezeichnung an, für die Sie den Verlauf anzeigen möchten.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history operation-show -profile PROFILE1 -label backup1
-verbose
```

Der Befehl Smo history purge

Mit diesem Befehl können Sie den Verlauf des SnapManager-Vorgangs löschen.

Syntax

```
        smo history purge
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

  Gibt den SnapManager-Vorgang an, für den Sie den Verlauf konfigurieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

Der Befehl smo history remove

Mit diesem Befehl können Sie den Verlauf der SnapManager-Vorgänge entfernen, die mit einem einzelnen Profil, mehreren Profilen oder allen Profilen in einem Repository verknüpft sind.

Syntax

```
        smo history remove
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[-password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name,
operation_name2\] \| -all\}
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

Gibt den SnapManager-Vorgang an, für den Sie den Verlauf konfigurieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history purge -profile -name PROFILE1 -operation
-operations backup
 -verbose
```

Der Befehl smo history set

Sie können den Befehl History Set ausführen, um die Vorgänge zu konfigurieren, für die Sie den Verlauf anzeigen möchten.

Syntax

```
        smo history set
-profile \{-name profile_name \[profile_name1, profile_name2\] \| -all
-repository
-login \[password repo_password\]
-username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation \{-operations operation_name \[operation_name1,
operation_name2\] \| -all\}
-retain
{-count retain_count \| -daily daily_count \| -monthly monthly_count \|
-weekly weekly_count}
[-quiet | -verbose]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Der Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Repository**

Gibt die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_dbname**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hosts an, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Port repo_Port**

  Gibt die Portnummer des Transmission Control Protocol (TCP) an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- *-Operation {-operationsOperation_Name [Operation_name1, Operation_name2]

  Gibt die SnapManager Vorgänge an, für die Sie den Verlauf konfigurieren möchten.

- **-contain {-countretain_count -dailytaily_count}**

  Legt die Aufbewahrungsklasse des Backups zur Erstellung fest, prüft Backup, Wiederherstellung und Wiederherstellung und erstellt Klonvorgänge. Die Aufbewahrungsklasse wird basierend auf der Anzahl der Vorgänge, der Anzahl der Tage, Wochen oder Monate festgelegt.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden Informationen zum Sicherungsvorgang angezeigt:

```
smo history set -profile -name PROFILE1 -operation -operations backup
-retain -daily 6
 -verbose
```

Der Befehl smo history show

Mit diesem Befehl können Sie detaillierte Verlaufsinformationen für ein bestimmtes Profil anzeigen.

Syntax

```
        smo history show
-profile profile
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

```
          smo  history show -profile -name PROFILE1
 -verbose
```

Der Befehl smo help

Sie können den Hilfe-Befehl ausführen, um Informationen zu den SnapManager-Befehlen und ihren Optionen anzuzeigen. Wenn Sie keinen Befehlsnamen angeben, wird eine Liste der gültigen Befehle angezeigt. Wenn Sie einen Befehlsnamen angeben, wird die Syntax für den Befehl angezeigt.

Syntax

```
        smo help
\[\]\[backup\|cmdfile\|clone\|credential\|help\|operation\|profile\|reposi
tory\|system\|version\|plugin\|diag\|history\|schedule\|notification\|stor
age\|get\]
\[-quiet \| -verbose\]
```

Parameter

Im Folgenden sind einige Befehlsnamen, die Sie mit diesem Befehl verwenden können:

- Backup
- Klon
- Cmdfile
- Anmeldedaten
- diag
- Get
- Benachrichtigung
- Hilfe
- Verlauf
- Betrieb
- Plug-in
- Profil
- Repository
- Zeitplan
- Storage
- System
- Version

Der Befehl smo notification remove-summary-notification

Mit diesem Befehl wird die Überblickbenachrichtigung für mehrere Profile in einer Repository-Datenbank deaktiviert.

Syntax

```
        smo notification remove-summary-notification
-repository
-dbname repo_service_name
-port repo_port
-host repo_host
-login -username repo_username
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login repo_username**

  Gibt den Anmeldenamen an, der für den Zugriff auf die Datenbank, in der das Repository gespeichert ist, erforderlich ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Im folgenden Beispiel wird die Überblickbenachrichtigung für mehrere Profile in einer Repository-Datenbank deaktiviert.

```
smo notification remove-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login -username oba5
```

Der Befehl smo notification Update-summary-notification

Sie können den Befehl Notification Update-summary-notification ausführen, um eine zusammenfassende Benachrichtigung für eine Repository-Datenbank zu aktivieren.

Syntax

```
        smo notification update-summary-notification
-repository
-port repo_port
-dbname  repo_service_name
-host repo_host
-login -username repo_username
-email email-address1,email-address2
-subject subject-pattern
-frequency
[-daily –time daily_time \|
-hourly –time hourly_time \|
-monthly –time monthly_time -date \[1\|2\|3\|...\|31\] \|
-weekly  –time weekly_time -day \[1\|2\|3\|4\|5\|6\|7\]\]
-profiles profile1,profile2
-notification-host notification-host
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Gibt die Details der Repository-Datenbank an.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- **-dbname repo_Service_Name**

  Gibt den Namen der Repository-Datenbank an. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hosts an, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an. Dies ist optional. Wenn nicht angegeben, verwendet SnapManager standardmäßig den Verbindungsmodus für OS-Authentifizierung.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Email-Adresse1, E-Mail-Adresse2**

  Gibt E-Mail-Adressen der Empfänger an.

- **-Betreff-Muster**

Gibt das Muster für E-Mail-Betreff an.

- **-Frequenz { -täglich --Zeit Tageszeit - stündlich --Zeit Stundenweise --Zeit monatlich --Zeit monatlich_Zeit -Datum {1 natürlich 3… 31 } --Zeit wöchentlich - Zeit wöchentlich - Tag {1 2 3 4 5 natürlich 6 7 } }**

  Gibt den Terminplantyp und die Zeitplandauer an, wann die E-Mail-Benachrichtigung angezeigt werden soll.

- **-Profile profil1, profil2**

  Gibt Profilnamen an, die E-Mail-Benachrichtigungen erfordern.

- **-notification-Host notification-Host**

  Gibt den SnapManager-Server-Host an, von dem aus die Zusammenfassung Benachrichtigungs-E-Mail an die Empfänger gesendet wird. Sie können Hostnamen oder IP-Adressen für den Benachrichtigungs-Host angeben. Sie können auch die Host-IP oder den Host-Namen aktualisieren.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Das folgende Beispiel ermöglicht eine zusammenfassende Benachrichtigung für eine Repository-Datenbank:

```
smo notification update-summary-notification –repository –port 1521
–dbname repo2 –host 10.72.197.133 –login –username oba5 –email
admin@org.com –subject success –frequency -daily -time 19:30:45 –profiles
sales1
```

Der Befehl smo notification set

Sie können den E-Mail-Server mit dem Befehl Notification Set konfigurieren.

Syntax

```
        smo notification set
-sender-email email_address
-mailhost mailhost
-mailport mailport
[-authentication
-username username
-password password]
-repository
-dbname repo_service_name
-port repo_port]
-host repo_host
-login -username repo_username
[-quiet | -verbose]
```

Parameter

- **-Absender-Email_address**

  Gibt die E-Mail-Adresse des Absenders an, von der die E-Mail-Benachrichtigungen gesendet werden. Ab SnapManager 3.2 für Oracle können Sie einen Bindestrich (-) einfügen, während Sie den Domain-Namen der E-Mail-Adresse angeben. Sie können beispielsweise die Absender-E-Mail-Adresse als -sender-email07lbfmdatacenter@continental-corporation.com angeben.

- **-mailhost mailhost**

  Gibt den Namen oder die IP-Adresse des Hostservers an, der E-Mail-Benachrichtigungen verarbeitet.

- **-mailport mailport**

  Gibt die Portnummer des Mail-Servers an.

- **-Authentifizierung -Benutzername -Passwort-Passwort**

  Gibt Authentifizierungsdetails für die E-Mail-Adresse an. Sie müssen Benutzernamen und Passwort angeben.

- **-Repository**

  Gibt die Details der Repository-Datenbank an.

- **-Port repo_Port**

  Gibt die Portnummer des Transmission Control Protocol (TCP) an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- **-dbname repo_Service_Name**

  Gibt den Namen der Repository-Datenbank an. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host repo_Host**

Gibt den Namen oder die IP-Adresse des Hosts an, auf dem sich die Repository-Datenbank befindet.

- **-Login**

  Gibt die Anmeldedaten für das Repository an. Dies ist optional. Wenn nicht angegeben, verwendet SnapManager standardmäßig den Verbindungsmodus für OS-Authentifizierung.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird der Mail-Server konfiguriert:

```
smo notification set -sender-email admin@org.com -mailhost
hostname.org.com -mailport 25 authentication -username davis -password
davis -repository -port 1521 -dbname SMOREPO -host hotspur
-login -username grabal21 -verbose
```

Der Befehl Smo Operation Dump

Sie können den Befehl Operation Dump ausführen, um eine JAR-Datei zu erstellen, die Diagnoseinformationen zu einem Vorgang enthält.

Syntax

```
        smo operation dump
-profile profile_name
\[-label label_name \| -id guid\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie die Speicherauszugsdateien erstellen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Label Label Label_Name**

Erstellt Dump-Dateien für den Vorgang und weist die angegebene Bezeichnung zu.

- **-id-Guid**

  Erstellt Dump-Dateien für den Vorgang mit der angegebenen GUID. Die GUID wird von SnapManager generiert, wenn der Vorgang beginnt.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird die Dump-Datei für das Backup erstellt:

```
smo operation dump -profile SALES1
-id 8abc01ec0e78f3e2010e78f3fdd00001
```

```
Dump file created Path:
C:\userhomedirectory\netapp\smo\3.3\smo_dump_8abc01ec0e78f3e2010e78f3fdd00
001.jar
```

Verwandte Informationen

Speicherauszug-Dateien

Befehl smo Operation list

Mit diesem Befehl werden die Zusammenfassungsinformationen aller Vorgänge aufgelistet, die für ein bestimmtes Profil aufgezeichnet wurden.

Syntax

```
        smo operation list
-profile profile_name
\[-delimiter character\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-Trennzeichen**

  (Optional) Wenn dieser Parameter angegeben wird, listet der Befehl jede Zeile in einer separaten Zeile auf und die Attribute in dieser Zeile werden durch das angegebene Zeichen getrennt.

- **-ruhig**

  (Optional) zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  (Optional) zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden die Zusammenfassungsinformationen aller Vorgänge aufgeführt, die mit dem angegebenen Profil protokolliert wurden.

```
smo operation list -profile myprofile
```

```
Start Date Status Operation ID Type Host
-------------------- ---------- --------------------------------
------------------ --
2007-07-16 16:03:57 SUCCESS 8abc01c813d0a1530113d0a15c5f0005 Profile
Create Host3
2007-07-16 16:04:55 FAILED 8abc01c813d0a2370113d0a241230001 Backup Host3
2007-07-16 16:50:56 SUCCESS 8abc01c813d0cc580113d0cc60ad0001 Profile
Update Host3
2007-07-30 15:44:30 SUCCESS 8abc01c81418a88e011418a8973e0001 Remove Backup
Host3
2007-08-10 14:31:27 SUCCESS 8abc01c814510ba20114510bac320001 Backup Host3
2007-08-10 14:34:43 SUCCESS 8abc01c814510e9f0114510ea98f0001 Mount Host3
2007-08-10 14:51:59 SUCCESS 8abc01c814511e6e0114511e78d40001 Unmount Host3
```

Verwandte Informationen

Anzeigen einer Liste von Vorgängen

Der Befehl smo Operation show

Sie können den Befehl „Operation show“ ausführen, um die Zusammenfassungsinformationen aller Vorgänge, die für das angegebene Profil durchgeführt wurden, aufzulisten. Die Ausgabe listet den Client-Benutzer (den Benutzer für den Client-PC) und den effektiven Benutzer (den Benutzer in SnapManager, der auf

dem ausgewählten Host gültig ist) auf.

Syntax

```
        smo operation show
-profile profile_name
\[-label label \| -id id\]
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- * Label*

  Gibt die Bezeichnung für den Vorgang an.

- **-id-id**

  Gibt die Kennung für den Vorgang an.

- **-ruhig**

  Optional: Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Optional: Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

In der folgenden Befehlszeile werden detaillierte Informationen über einen Vorgang angezeigt:

```
# smo operation show -profile myprofile -id
ff8080811295eb1c011295eb28230001
```

```
Operation Attempted
   Operation ID: ff8080811295eb1c011295eb28230001
   Type:RestoreFor profile: myprofile
   With Force: No
   Performed on backup
   Operation ID: ff8080811295eb1c011296eb23290001
   Label: mylabel
Operation Runtime Information
   Status: SUCCESS
   Start date: 2007-07-16 13:24:09 IST
   End date: 2007-07-16 14:10:10 IST
   Client user: amorrow
   Effective user: amorrow
Host
   Host Run upon: Host3
   Process ID: 3122
   SnapManager version: 3.3
Repository
   Connection: user1@SMOREPO/hotspur:1521
   Repository version: 3.3
Resources in use
   Volume:
     ssys1:/vol/luke_ES0_0 (FlexClone)
   Filesystems:C:\\SnapManager_auto_mounts\\O-20120712052511170_0
```

Verwandte Informationen

Anzeigen von Betriebsdetails

Der Befehl smo password Reset

Sie können den Befehl zum Zurücksetzen des Passworts ein Profil zurücksetzen.

Syntax

```
        smo password reset
-profile profile
\[-profile-password profile_password\]
\[-repository-hostadmin-password repository_hostadmin_password\]
[-quiet | -verbose]
```

Parameter

- **-Profil**

Gibt den Namen des Profils an, für das Sie das Passwort zurücksetzen möchten.

- **-profile-password Profil_password**

  Gibt das neue Kennwort für das Profil an.

- **-Repository-hostadmin-password admin_password**

  Gibt die autorisierten Benutzerberechtigungen mit lokaler Administratorberechtigung für die Repository-Datenbank an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Der Befehl smo profile create

Sie können den Befehl Profile create ausführen, um ein Profil einer Datenbank in einem Repository zu erstellen. Sie müssen die Datenbank mounten, bevor Sie diesen Befehl ausführen.

Syntax

```
        smo profile create
-profile profile
\[-profile-password profile_password\]
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database
-dbname db_dbname
-host db_host
[-sid  db_sid\]
[-login
\[-username db_username -password db_password -port db_port\]
 ]
[-rman \{-controlfile \| \{-login
-username  rman_username -password  rman_password\}
-tnsname  rman_tnsname\}\}]


[-retain
```

```
\[-hourly \[-count n\] \[-duration m\]\]
\[-daily \[-count n\] \[-duration m\]]
\[-weekly \[-count n\] \[-duration m\]]
\[-monthly \[-count n\] \[-duration m\]]]]
-comment comment
-snapname-pattern pattern
[]
[-summary-notification]
[-notification
\[-success
-email email_address1,email_address2
-subject subject_pattern\]
\[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups
-retain-archivelog-backups
 -hours hours |
-days days |
-weeks weeks |
-months months
[]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
[-quiet | -verbose]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-profile-password Profil_password**

  Geben Sie das Kennwort für das Profil an.

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank an, in der das Profil gespeichert wird.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Profil gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank

ausgeführt wird.

- **-sid db_sid**

  Gibt die Systemkennung der Datenbank an, die das Profil beschreibt. Standardmäßig verwendet SnapManager den Datenbanknamen als Systemkennung. Falls sich die Systemkennung vom Datenbanknamen unterscheidet, müssen Sie sie mit der Option -sid angeben.

- **-Login**

  Gibt die Anmeldedaten für das Repository an.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Repository-Datenbank verwendet wird.

- **-Datenbank**

  Gibt die Details der Datenbank an, die das Profil beschreibt. Diese Datenbank wird gesichert, wiederhergestellt und geklont.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host db_Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Datenbank ausgeführt wird.

- **-Login**

  Gibt die Anmeldedaten für die Datenbank an.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Port db_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, die das Profil beschreibt.

- **-rman**

  Gibt die Details an, die SnapManager zum Katalogisieren von Backups mit dem Oracle Recovery Manager (RMAN) verwendet.

- **-controlfile**

  Gibt die Steuerdateien für die Zieldatenbank an, anstatt einen Katalog als RMAN-Repository zu verwenden.

- **-Login**

  Gibt die RMAN-Anmeldedaten an.

- **-Passwort rman_password**

  Gibt das Kennwort an, mit dem Sie sich beim RMAN-Katalog anmelden können.

- **-username rman_Benutzername**

  Gibt den Benutzernamen an, der zum Anmelden beim RMAN-Katalog verwendet wird.

- **-tnsname tnsname**

  Gibt den Verbindungsnamen tnsname an (dieser wird in der Datei tsname.ora definiert).

- **-halten [-hourly [-count n] [-duration m] [-taily [-count n] [-duration m]] [-Weekly [-count n] [-duration m]] [-monthly [-count n] [-duration m]]**

  Gibt die Aufbewahrungsrichtlinie für ein Backup an, bei dem entweder oder beide Aufbewahrungsdaten zusammen mit einer Aufbewahrungsdauer für eine Aufbewahrungsklasse (stündlich, täglich, wöchentlich, monatlich) zählen.

  Für jede Aufbewahrungsklasse kann entweder oder beides einer Anzahl von Aufbewahrungsfristen oder eine Aufbewahrungsdauer angegeben werden. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunde, Tage für Tag). Wenn der Benutzer beispielsweise nur eine Aufbewahrungsdauer von 7 für tägliche Backups angibt, dann wird SnapManager nicht die Anzahl der täglichen Backups für das Profil begrenzen (da die Aufbewahrungsanzahl 0 ist), aber SnapManager löscht automatisch täglich erstellte Backups, die vor 7 Tagen erstellt wurden.

- **-Kommentar**

  Gibt den Kommentar für ein Profil an, das die Profildomäne beschreibt.

- **-snapname-Muster**

  Gibt das Benennungsmuster für Snapshot Kopien an. Außerdem können Sie in allen Namen von Snapshot Kopien benutzerdefinierten Text einfügen, beispielsweise HAOPS für hochverfügbare Vorgänge. Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht erstellt wurden. Snapshot Kopien, die vorhanden sind, behalten das vorherige SnapName-Muster bei. Sie können mehrere Variablen im Mustertext verwenden.

- **-summary-notification**

  Gibt an, dass die E-Mail-Benachrichtigung für das neue Profil aktiviert ist.

- **-notification -success-email e-Mail_adress1,E-Mail address2 -subject_pattern**

  Gibt an, dass die E-Mail-Benachrichtigung für das neue Profil aktiviert ist, so dass E-Mails von Empfängern empfangen werden, wenn der SnapManager-Vorgang erfolgreich ist. Sie müssen eine einzelne E-Mail-

Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den E-Mail-Betreff für das neue Profil.

Sie können auch benutzerdefinierten Subjekttext für das neue Profil einfügen. Sie können den Betreff ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-notification -Failure -Email-Mail_adress1,E-Mail address2 -subject_pattern**

  Gibt an, dass die E-Mail-Benachrichtigung aktivieren für das neue Profil aktiviert ist, damit E-Mails von Empfängern empfangen werden, wenn der SnapManager-Vorgang fehlschlägt. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den E-Mail-Betreff für das neue Profil.

  Sie können auch benutzerdefinierten Subjekttext für das neue Profil einfügen. Sie können den Betreff ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-separate-archivlog-Backups**

  Gibt an, dass die Backup des Archivprotokolls von der Datendatei-Sicherung getrennt ist. Dies ist ein optionaler Parameter, den Sie beim Erstellen des Profils angeben können. Nachdem Sie die Sicherung mit dieser Option getrennt haben, können Sie entweder Datendateien-only-Backup oder Archiv-Log-only-Backup machen.

- **-behalten-archivelog-Backups -Stunden- -Tage- Wochen- Monthsmonths**

  Gibt an, dass die Archiv-Log-Backups auf Basis der Aufbewahrungsdauer des Archivprotokolls aufbewahrt werden (stündlich, täglich, wöchentlich, monatlich).

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

- **-include-with-online-Backups**

  Gibt an, dass das Backup des Archivprotokolls zusammen mit dem Online-Datenbank-Backup enthalten ist.

- **-no-include-with-online-Backups**

  Gibt an, dass die Archiv-Log-Backups nicht zusammen mit dem Online-Datenbank-Backup enthalten sind.

- **-dump**

  Gibt an, dass die Dump-Dateien nach dem erfolgreichen Erstellen des Profils gesammelt werden.

Beispiel

Das folgende Beispiel zeigt die Erstellung eines Profils mit stündlicher Aufbewahrungsrichtlinie und E-Mail-

Benachrichtigung:

```
smo profile create -profile test_rbac -profile-password netapp -repository
-dbname SMOREP -host hostname.org.com -port 1521 -login -username smorep
-database -dbname
RACB -host saal -sid racb1 -login -username sys -password netapp -port
1521 -rman -controlfile -retain -hourly -count 30 -verbose
Operation Id [8abc01ec0e78ebda010e78ebe6a40005] succeeded.
```

Verwandte Informationen

Profilverwaltung für effiziente Backups

Benennen von Snapshot-Kopien

Wie SnapManager Backups auf dem lokalen Storage aufbewahrt

Der Befehl smoprofile delete

Sie können den Befehl „Profil löschen“ ausführen, um ein Profil der Datenbank zu löschen.

Syntax

```
        smo profile delete
-profile profile
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt das zu löschende Profil an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Profil gelöscht:

```
smo profile delete -profile SALES1
Operation Id [Ncaf00af0242b3e8dba5c68a57a5ae932] succeeded.
```

Verwandte Informationen

Profile werden gelöscht

Der Befehl smoprofile dump

Sie können den Profildump-Befehl ausführen, um die .jar-Datei zu erstellen, die Diagnoseinformationen zu einem Profil enthält.

Syntax

```
        smo profile dump
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt das Profil an, für das Sie die Speicherauszugsdateien erstellen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird ein Dump für das Profil SALES1 erstellt:

```
smo profile dump -profile SALES1
Dump file created
Path:
C:\\userhomedirectory\\netapp\\smo\\3.3.0\\smo_dump_SALES1_hostname.jar
```

Der Befehl smo profile list

Mit diesem Befehl wird eine Liste der aktuellen Profile angezeigt.

Syntax

```
        smo profile list
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Im folgenden Beispiel werden vorhandene Profile mit ihren Details angezeigt.

```
smo profile list -verbose
Profile name: FGTER
Repository:
  Database name: SMOREPO
  SID: SMOREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: ********
Profile name: TEST_RBAC
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: TEST_RBAC_DP_PROTECT
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: TEST_HOSTCREDEN_OFF
Repository:
```

```
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: SMK_PRF
Repository:
  Database name: smorep
  SID: smorep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smosaal
  Password: ********
Profile name: FGLEX
Repository:
  Database name: SMOREPO
  SID: SMOREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: ********
```

Der Befehl smo profile show

Sie können den Befehl „Profile show“ ausführen, um die Informationen zu einem Profil anzuzeigen.

Syntax

```
        smo profile show
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Der Befehl smo profile SYNC

Mit diesem Befehl werden die Profile-to-Repository-Zuordnungen für dieses Repository in eine Datei im Home-Verzeichnis auf dem lokalen Host geladen.

Syntax

```
        smo profile sync
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login
-username repo_username
               \[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt die Repository-Datenbank für das zu synchronisierende Profil an.

- **-Host**

  Gibt den Datenbank-Host an.

- **-Port**

  Gibt den Port für den Host an.

- **-Login**

  Gibt den Anmeldeprozess für den Hostbenutzer an.

- **-username**

  Gibt den Benutzernamen für den Host an.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel zeigt das Ergebnis des Befehls zum Synchronisieren der Profile-zu-Repository-Zuordnungen für die Datenbank.

```
smo profile sync -repository -dbname smrepo -host Host2 -port 1521 -login
-username user2
SMO-12345 [INFO ]: Loading profile mappings for repository
"user2@Host2:smrepo" into cache for OS User "admin".
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

Der Befehl smoprofile Update

Sie können den Befehl „Profilaktualisierung“ ausführen, um die Informationen für ein vorhandenes Profil zu aktualisieren.

Syntax

```
        smo profile update
-profile profile
\[-new-profile new_profile_name\]
\[-profile-password profile_password\]
[-database
-dbname db_dbname
-host db_host
\[-sid db_sid\]
[-login
\[-username db_username -password db_password -port db_port\]
 ]
[\{-rman  \{-controlfile \| \{\{-login
-username  rman_username
-password  rman_password \}
\[-tnsname  tnsname\]\}\}\} \|
-remove-rman\]


[-retain
\[-hourly \[-count n\] \[-duration m\]\]
\[-daily \[-count n\] \[-duration m\]]
\[-weekly \[-count n\] \[-duration m\]]
\[-monthly \[-count n\] \[-duration m\]]]]
-comment comment
-snapname-patternpattern
[]
[-summary-notification]
[-notification
\[-success
-email email_address1,email_address2
-subject subject_pattern\]
\[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups
-retain-archivelog-backups
-hours  hours |
-days days |
-weeks weeks |
-months months
[]
[-include-with-online-backups \| -no-include-with-online-backups]]
[-dump]
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-profile-password Profil_password**

  Gibt das Kennwort für das Profil an.

- **-New-profile New_profile_Name**

  Gibt den neuen Namen an, den Sie für ein Profil angeben können.

- **-Datenbank**

  Gibt die Details der Datenbank an, die das Profil beschreibt. Diese Datenbank wird gesichert, wiederhergestellt usw.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Datenbank ausgeführt wird.

- **-sid db_sid**

  Gibt die Systemkennung der Datenbank an, die das Profil beschreibt. Standardmäßig verwendet SnapManager den Datenbanknamen als Systemkennung. Falls sich die Systemkennung vom Datenbanknamen unterscheidet, müssen Sie sie mit der Option -sid angeben.

- **-Login**

  Gibt die Anmeldedaten für das Repository an.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Repository-Datenbank erforderlich ist.

- **-Datenbank**

  Gibt die Details der Datenbank an, die das Profil beschreibt. Diese Datenbank wird gesichert, wiederhergestellt und geklont.

- **-dbname db_dbname**

  Gibt den Namen der Datenbank an, die das Profil beschreibt. Sie können entweder den globalen Namen oder die Systemkennung verwenden.

- **-Host db_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Datenbank ausgeführt wird.

- **-Login**

  Gibt die Anmeldedaten für die Datenbank an.

- **-username db_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Passwort db_password**

  Gibt das Kennwort an, das für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-Port db_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank erforderlich ist, die das Profil beschreibt.

- **-rman**

  Gibt die Details an, die SnapManager zum Katalogisieren von Backups mit dem Oracle Recovery Manager (RMAN) verwendet.

- **-controlfile**

  Gibt die Steuerdateien für die Zieldatenbank an, anstatt einen Katalog als RMAN-Repository zu verwenden.

- **-Login**

  Gibt die RMAN-Anmeldedaten an.

- **-Passwort rman_password**

  Gibt das Kennwort an, mit dem Sie sich beim RMAN-Katalog anmelden können.

- **-username rman_Benutzername**

  Gibt den Benutzernamen an, der zum Anmelden beim RMAN-Katalog verwendet wird.

- **-tnsname tnsname**

  Gibt den Verbindungsnamen tnsname an (dieser wird in der Datei tsname.ora definiert).

- **-remove-rman**

  Legt fest, dass RMAN im Profil entfernt wird.

- **-behalten [-hourly [-countn] [-duration m] [-taily [-count n] [-duration m]] [-Weekly [-count n][-duration m]] [-monthly [-count n][-duration m]]**

  Gibt die Aufbewahrungsklasse (stündlich, täglich, wöchentlich, monatlich) für ein Backup an.

Für jede Aufbewahrungsklasse kann ein Aufbewahrungszähler oder eine Aufbewahrungsdauer oder beides angegeben werden. Die Dauer ist in Einheiten der Klasse (z. B. Stunden für Stunden oder Tage für täglich). Wenn der Benutzer beispielsweise nur eine Aufbewahrungsdauer von 7 für tägliche Backups angibt, dann wird SnapManager nicht die Anzahl der täglichen Backups für das Profil begrenzen (da die Aufbewahrungsanzahl 0 ist), aber SnapManager löscht automatisch täglich erstellte Backups, die vor 7 Tagen erstellt wurden.

- **-Kommentar**

  Gibt den Kommentar für ein Profil an.

- **-snapname-Muster**

  Gibt das Benennungsmuster für Snapshot Kopien an. Außerdem können Sie in allen Namen von Snapshot Kopien benutzerdefinierten Text einfügen, beispielsweise HAOPS für hochverfügbare Vorgänge. Sie können das Benennungsmuster der Snapshot Kopie ändern, wenn Sie ein Profil erstellen oder nachdem das Profil erstellt wurde. Das aktualisierte Muster gilt nur für Snapshot Kopien, die noch nicht aufgetreten sind. Snapshot Kopien, die vorhanden sind, behalten das vorherige SnapName-Muster bei. Sie können mehrere Variablen im Mustertext verwenden.

- **-summary-notification**

  Gibt an, dass die E-Mail-Benachrichtigung für das vorhandene Profil aktiviert ist.

- **-Mitteilung [-success-email e-Mail_adress1,E-Mail address2 -subject_pattern]**

  Aktiviert die E-Mail-Benachrichtigung für das vorhandene Profil, sodass die Empfänger nach erfolgreicher SnapManager-Operation E-Mails erhalten. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den Betreff der E-Mail für das vorhandene Profil.

  Sie können den Betreff während der Aktualisierung des Profils ändern oder benutzerdefinierten Text einfügen. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-Benachrichtigung [-Failure -Email-adress1,E-Mail address2 -subject_pattern]**

  Aktiviert die E-Mail-Benachrichtigung für das vorhandene Profil, sodass die Empfänger bei Ausfall des SnapManager-Vorgangs E-Mails erhalten. Sie müssen eine einzelne E-Mail-Adresse oder mehrere E-Mail-Adressen eingeben, an die E-Mail-Benachrichtigungen gesendet werden, sowie ein Muster für den Betreff der E-Mail für das vorhandene Profil.

  Sie können den Betreff während der Aktualisierung des Profils ändern oder benutzerdefinierten Text einfügen. Der aktualisierte Betreff gilt nur für die nicht gesendeten E-Mails. Sie können mehrere Variablen für den E-Mail-Betreff verwenden.

- **-separate-archivlog-Backups**

  Trennt das Backup des Archivprotokolls von der Datendatei-Sicherung. Dies ist ein optionaler Parameter, den Sie beim Erstellen des Profils angeben können. Nachdem Sie die Backups mit dieser Option getrennt haben, können Sie entweder Datendateien-only-Backup oder Archiv-Log-only-Backup erstellen.

- **-behalten-archivelog-Backups -Stunden- -Tage- Wochen- Monthsmonths**

  Gibt an, dass die Archiv-Log-Backups auf Basis der Aufbewahrungsdauer des Archivprotokolls aufbewahrt

werden (stündlich, täglich, wöchentlich, monatlich).

- **-enthalten-mit-online-Backups**

  Gibt an, dass das Backup des Archivprotokolls zusammen mit dem Online-Datenbank-Backup enthalten ist.

  Gibt an, dass die Archiv-Log-Backups nicht zusammen mit dem Online-Datenbank-Backup enthalten sind.

- **-dump**

  Gibt an, dass die Dump-Dateien nach dem erfolgreichen Erstellen des Profils gesammelt werden.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel werden die Anmeldeinformationen für die im Profil beschriebene Datenbank geändert und die E-Mail-Benachrichtigung ist für dieses Profil konfiguriert:

```
smo profile update -profile SALES1 -database -dbname SALESDB
 -sid SALESDB -login -username admin2 -password d4jPe7bw -port 1521
-host server1 -profile-notification -success -e-mail Preston.Davis@org.com
-subject success
Operation Id [8abc01ec0e78ec33010e78ec3b410001] succeeded.
```

Verwandte Informationen

Profilkennwörter werden geändert

Wie SnapManager Backups auf dem lokalen Storage aufbewahrt

Der Befehl smoprofile verify

Sie können den Befehl „Profile Verify“ ausführen, um die Einrichtung des Profils zu überprüfen. Sie müssen die Datenbank mounten, bevor Sie diesen Befehl ausführen.

Syntax

```
        smo profile verify
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt das zu überprüfenden Profil an. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird das Profil überprüft:

```
smo profile verify -profile profileA -verbose
 [ INFO] SMO-13505: SnapDrive environment verification passed.
[ INFO] SMO-13507: JDBC verification for "OS authenticated:
NEWDB/hostA.rtp.com" passed.
[ INFO] SMO-13506: SQLPlus verification for database SID "NEWDB" passed.
Environment: [ORACLE_HOME=E:\app\Administrator\product\11.2.0\dbhome_1]
[ INFO] SMO-07431: Saving starting state of the database:
Database[NEWDB(OPEN)], Service[RUNNING].
[ INFO] SMO-07431: Saving starting state of the database:
Database[NEWDB(OPEN)], Service[RUNNING].
[ INFO] SD-00016: Discovering storage resources for F:\.
[ INFO] SD-00017: Finished storage discovery for F:\.
[ INFO] SD-00016: Discovering storage resources for F:\.
[ INFO] SD-00017: Finished storage discovery for F:\.
[ INFO] SD-00016: Discovering storage resources for H:\.
[ INFO] SD-00017: Finished storage discovery for H:\.
[ INFO] SD-00016: Discovering storage resources for G:\.
[ INFO] SD-00017: Finished storage discovery for G:\.
[ INFO] SD-00016: Discovering storage resources for I:\.
[ INFO] SD-00017: Finished storage discovery for I:\.
[ WARN] SMO-05071: Database profile HADLEY is not eligible for fast
restore:  Restore Plan:
  Preview:

    The following components will be restored completely via: host side
file copy restore
      F:\NEWDB\SYSAUX01.DBF
      F:\NEWDB\SYSTEM01.DBF
      F:\NEWDB\UNDOTBS01.DBF
```

```
      F:\NEWDB\USERS01.DBF

  Analysis:

    The following reasons prevent certain components from being restored
completely via: storage side file system restore
      * Files in file system F:\ not part of the restore scope will be
reverted.
    Components not in restore scope:
      F:\_TESTCLN\CONTROL01.CTL
      F:\_TESTCLN\REDO_1.LOG
      F:\_TESTCLN\REDO_2.LOG
      F:\_TESTCLN\REDO_3.LOG
    Components to restore:
      F:\NEWDB\SYSAUX01.DBF
      F:\NEWDB\SYSTEM01.DBF
      F:\NEWDB\UNDOTBS01.DBF
      F:\NEWDB\USERS01.DBF

  * Reasons denoted with an asterisk (*) are overridable.

[ INFO] SMO-07433: Returning the database to its initial state: Database
[NEWDB(OPEN)], Service[RUNNING].
[ INFO] SMO-13048: Profile Verify Operation Status: SUCCESS
[ INFO] SMO-13049: Elapsed Time: 0:19:06.949
Operation Id [N5bc18bd5c3be27a795ce3857093a926a] succeeded.
```

Verwandte Informationen

Profile werden überprüft

Der Befehl smo Repository create

Syntax

Mit diesem Befehl wird ein Repository erstellt, in dem Datenbankprofile und zugehörige Anmeldedaten gespeichert werden. Dieser Befehl überprüft außerdem, ob die Blockgröße geeignet ist.

```
        smo repository create
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Erstellung des Repositorys zu erzwingen. Wenn Sie diese Option verwenden, werden Sie von SnapManager aufgefordert, das Repository zu sichern, bevor Sie das Repository erstellen.

- **-noprompt**

  Zeigt nicht die Aufforderung zum Sichern des Repository vor der Erstellung an, wenn Sie die Option -Force verwenden. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert das Erstellen von Repositories mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Befehlsbeispiel

Im folgenden Beispiel wird ein Repository in der Datenbank SMOREPO auf dem Host hotspur erstellt.

```
smo repository create -repository -port 1521 -dbname SMOREPO -host hotspur
-login -username grabal21 -verbose
SMO-09202 [INFO ]: Creating new schema as grabal21 on
jdbc:oracle:thin:@//hotspur:1521/SMOREPO.
SMO-09205 [INFO ]: Schema generation complete.
SMO-09209 [INFO ]: Performing repository version INSERT.
SMO-09210 [INFO ]: Repository created with version: 30
SMO-13037 [INFO ]: Successfully completed operation: Repository Create
SMO-13049 [INFO ]: Elapsed Time: 0:00:08.844
```

Verwandte Informationen

Repositories werden erstellt

Der Befehl smo Repository löschen

Mit diesem Befehl wird ein Repository gelöscht, das zum Speichern von Datenbankprofilen und zugehörigen Anmeldedaten verwendet wird. Sie können ein Repository nur löschen, wenn kein Profil im Repository vorhanden ist.

Syntax

```
        smo repository delete
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Force**

  Versucht, das Löschen des Repositorys zu erzwingen, auch wenn unvollständige Vorgänge vorliegen. SnapManager gibt eine Eingabeaufforderung aus, wenn unvollständige Vorgänge vorliegen. Sie werden gefragt, ob Sie das Repository wirklich löschen möchten.

- **-noprompt**

  Fordert Sie nicht auf, bevor Sie das Repository löschen. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert das Löschen von Repositorys mit einem Skript.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Befehlsbeispiel

Im folgenden Beispiel wird das Repository in der SALESDB-Datenbank gelöscht.

```
smo repository delete -repository -port 1521 -dbname smorep
-host nila -login -username smofresno -force -verbose
This command will delete repository "smofresno@smorep/nila".
Any resources maintained by the repository must be cleaned up manually.
This may include snapshots, mounted backups, and clones.
Are you sure you wish to proceed (Y/N)?Y
[ INFO] SMO-09201: Dropping existing schema as smofresno
  on jdbc:oracle:thin:@//nila:1521/smorep.
[ INFO] SMO-13048: Repository Delete Operation Status: SUCCESS
[ INFO] SMO-13049: Elapsed Time: 0:00:06.372
[ INFO] SMO-20010: Synchronizing mapping for profiles in
   repository "smofresno@smorep/nila:1521".
[ WARN] SMO-20029: No repository schema exists in
"smofresno@smorep/nila:1521".
 Deleting all profile mappings for this repository.
[ INFO] SMO-20012: Deleted stale mapping for profile "TESTPASS".
```

Der smo Repository Rollback-Befehl

Mit diesem Befehl können Sie ein Rollback bzw. ein Wechsel von einer höheren Version von SnapManager zu der Originalversion, von der Sie ein Upgrade durchgeführt haben, durchführen.

Syntax

```
        smo repository rollback
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-rollbackhost host_with_target_database
[-force]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-rollbackhost Host_with_target_Database**

  Gibt den Namen des Hosts an, der von einer höheren Version von SnapManager auf die ursprüngliche niedrigere Version zurückgesetzt wird.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Aktualisierung des Repositorys zu erzwingen. SnapManager fordert Sie auf, vor der Aktualisierung eine Sicherung des aktuellen Repository durchzuführen.

- **-noprompt**

  Zeigt die Eingabeaufforderung nicht an, bevor die Repository-Datenbank aktualisiert wird. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert die Aktualisierung von Repositorys mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel aktualisiert das Repository in der SALESDB-Datenbank.

```
smo repository rollback -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -rollbackhost hostA
```

Der Befehl smo Repository rollingupgrade

Mit diesem Befehl wird das Upgrade auf einen einzelnen oder mehrere Hosts und die zugehörigen Zieldatenbanken durchgeführt – von einer niedrigeren Version von SnapManager auf eine höhere Version. Der aktualisierte Host wird nur mit der höheren Version von SnapManager verwaltet.

Syntax

```
        smo repository rollingupgrade
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-upgradehost host_with_target_database
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Upgradehost Host_with_Target_Database**

  Gibt den Namen des Hosts an, der von einer niedrigeren Version von SnapManager auf eine höhere Version aktualisiert wird.

- **-Port repo_Port**

Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Aktualisierung des Repositorys zu erzwingen. SnapManager fordert Sie auf, vor der Aktualisierung eine Sicherung des aktuellen Repository durchzuführen.

- **-noprompt**

  Zeigt die Eingabeaufforderung nicht an, bevor die Repository-Datenbank aktualisiert wird. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert die Aktualisierung von Repositorys mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel aktualisiert das Repository in der SALESDB-Datenbank.

```
smo repository rollingupgrade -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -upgradehost hostA
```

Der Befehl smo Repository show

Mit diesem Befehl werden Informationen zum Repository angezeigt.

Syntax

```
        smo repository show
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Befehlsbeispiel

Das folgende Beispiel zeigt Details zum Repository in der SALESDB-Datenbank.

```
smo repository show -repository -dbname SALESDB -host server1
-port 1521 -login -username admin
Repository Definition:
User Name: admin
Host Name: server1
Database Name: SALESDB
Database Port: 1521
Version: 28
Hosts that have run operations using this repository: 2
server2
server3
Profiles defined in this repository: 2
GSF5A
GSF3A
Incomplete Operations: 0
```

Der Befehl smo Repository Update

Mit diesem Befehl wird das Repository aktualisiert, in dem Datenbankprofile und die zugehörigen Anmeldedaten gespeichert werden, wenn Sie ein SnapManager-Upgrade durchführen. Wenn Sie eine neue Version von SnapManager installieren, müssen Sie den Befehl Repository Update ausführen, bevor Sie die neue Version verwenden können. Sie können diesen Befehl nur verwenden, wenn im Repository keine unvollständigen Befehle vorhanden sind.

Syntax

```
        smo repository update
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
[-force] [-noprompt]
\[-quiet \| -verbose\]
```

Parameter

- **-Repository**

  Die Optionen, die dem -Repository folgen, geben die Details der Datenbank für das Repository an.

- **-dbname repo_Service_Name**

  Gibt den Namen der Datenbank an, in der das Repository gespeichert wird. Verwenden Sie entweder den

globalen Namen oder den SID.

- **-Host repo_Host**

  Gibt den Namen oder die IP-Adresse des Hostcomputers an, auf dem die Repository-Datenbank ausgeführt wird.

- **-Login**

  Startet die Repository-Anmeldedaten.

- **-username repo_username**

  Gibt den Benutzernamen an, der für den Zugriff auf die Datenbank erforderlich ist, in der das Repository gespeichert ist.

- **-Port repo_Port**

  Gibt die TCP-Portnummer an, die für den Zugriff auf die Datenbank verwendet wird, in der das Repository gespeichert ist.

- **-Force**

  Versucht, die Aktualisierung des Repositorys zu erzwingen. SnapManager fordert Sie auf, vor der Aktualisierung eine Sicherung des aktuellen Repository durchzuführen.

- **-noprompt**

  Zeigt die Eingabeaufforderung nicht an, bevor die Repository-Datenbank aktualisiert wird. Mit der Option -noprompt wird sichergestellt, dass die Eingabeaufforderung nicht angezeigt wird. Dies erleichtert die Aktualisierung von Repositorys mithilfe eines Skripts.

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispielbefehl

Das folgende Beispiel aktualisiert das Repository in der SALESDB-Datenbank.

```
smo repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521
```

Der Befehl smo schedule create

Sie können mit dem Befehl „Schedule create“ ein Backup zu einem bestimmten Zeitpunkt planen.

Syntax

```
        smo schedule create
-profile profile_name
\[-full\{-auto \| -online \| -offline\}
\[-retain -hourly \| -daily \| -weekly \| -monthly \| -unlimited\]
\[-verify\]\] |
\[-data \[\[-files files \[files\]\] \|
\[-tablespaces tablespaces \[tablespaces\]\] \{-auto \| -online \|
-offline\}
\[-retain -hourly \| -daily \| -weekly \| -monthly \| -unlimited\]
\[-verify\]\] |
\[-archivelogs\]}
\[-label label\]
\[-comment comment\]

\[-backup-dest path1 \[ , path2\]\]
\[-exclude-dest path1 \[ , path2\]\]
\[-prunelogs \{-all \| -until-scn until-scn \| -until -date  yyyy-MM-
dd:HH:mm:ss\] \| -before \{-months \| -days \| -weeks \| -hours}}
-prune-dest prune_dest1,\[prune_dest2\]\]
-schedule-name schedule_name
\[-schedule-comment schedule_comment\]
-interval \{-hourly \| -daily \| -weekly \| -monthly \| -onetimeonly\}
-cronstring cron_string
-start-time \{start_time <yyyy-MM-dd HH:mm\>\}
-runasuser runasuser
\[-taskspec taskspec\]
-force
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, für die das Backup geplant werden soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Auto Option**

  Wenn die Datenbank im Status „angehängt“ oder „Offline“ steht, führt SnapManager ein Offline-Backup durch. Wenn sich die Datenbank im offenen oder Online-Status befindet, führt SnapManager ein Online-Backup durch. Wenn Sie die Option -Force mit der Option -offline verwenden, erzwingt SnapManager ein Offline-Backup, selbst wenn die Datenbank derzeit online ist.

- **-Online-Option**

  Gibt ein Online-Datenbank-Backup an.

- **-Offline-Option**

  Gibt eine Offline-Sicherung an, während sich die Datenbank im Shutdown-Status befindet. Wenn sich die Datenbank im offenen oder gemounteten Status befindet, schlägt das Backup fehl. Wenn die Option -Force verwendet wird, versucht SnapManager, den Datenbankstatus zu ändern, um die Datenbank für ein Offline-Backup herunterzufahren.

- **-Volloption**

  Sicherung der gesamten Datenbank. Dazu gehören alle Daten, archivierte Log- und Kontrolldateien. Die archivierten Wiederherstellungsprotokolle und Kontrolldateien werden gesichert, unabhängig davon, welche Art von Backup Sie durchführen. Wenn Sie nur einen Teil der Datenbank sichern möchten, verwenden Sie die Option -files oder -Tablespaces.

- **-Dateiliste**

  Sichert nur die angegebenen Datendateien sowie die archivierten Protokoll- und Kontrolldateien. Trennen Sie die Liste der Dateinamen mit Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * -Tablespaces*

  Sicherung nur der angegebenen Datenbanktablespaces plus der archivierten Protokoll- und Kontrolldateien Trennen Sie die Namen der Tablespaces durch Leerzeichen. Wenn die Datenbank offen ist, überprüft SnapManager, ob sich die entsprechenden Tabellen im Online-Backup-Modus befinden.

- * Name des Etiketts*

  Gibt einen optionalen Namen für dieses Backup an. Dieser Name muss innerhalb des Profils eindeutig sein. Der Name kann Buchstaben, Zahlen, Unterstrich (_) und Bindestrich (-) enthalten. Es kann nicht mit einem Bindestrich beginnen.

  Wenn Sie keine Beschriftung angeben, erstellt SnapManager im Scope_type_date-Format eine Standardbeschriftung:

  - Der Umfang ist entweder F, um ein vollständiges Backup anzuzeigen, oder P, um auf ein teilweises Backup hinzuweisen.
  - Geben Sie C ein, um ein Offline-Backup (Cold) anzuzeigen, H für ein Online-Backup (Hot) oder Ein Für die automatische Sicherung, z. B. P_A_20081010060037IST, anzuzeigen.
  - Datum ist Jahr, Monat, Tag und Uhrzeit des Backups.

    SnapManager verwendet eine 24-Stunden-Zeit.

  Beispiel: Wenn Sie am 16. Januar 2007 um 5:45:16 Uhr eine vollständige Sicherung mit offline der Datenbank durchgeführt haben Eastern Standard Time, SnapManager würde die Bezeichnung F_C_20070116174516EST erstellen.

- **-comment-Zeichenfolge**

  Gibt einen optionalen Kommentar an, um dieses Backup zu beschreiben. Schließen Sie den String in einzelne Anführungszeichen (').

Einige Schalen Streifen Anführungszeichen ab. Wenn dies für Ihre Shell zutrifft, müssen Sie das Anführungszeichen mit einem umgekehrten Schrägstrich (\) angeben. Beispielsweise müssen Sie Folgendes eingeben: `\' this is a comment\'`.

- **-Verify Option**

  Überprüft, ob die Dateien im Backup nicht beschädigt sind, indem Sie das Oracle dbv-Dienstprogramm ausführen.

  Wenn Sie die Option -verify angeben, wird der Backup-Vorgang erst abgeschlossen, wenn der Überprüfungvorgang abgeschlossen ist.

- **-Force Option**

  Erzwingt eine Statusänderung, wenn sich die Datenbank nicht im richtigen Zustand befindet. Beispielsweise kann SnapManager den Status der Datenbank von Online- in Offline-Modus ändern, basierend auf dem von Ihnen angegebenen Backup-Typ und dem Status, in dem sich die Datenbank befindet.

  - Wenn die lokale Instanz sich im Shutdown-Status befindet und mindestens eine Instanz geöffnet ist, können Sie die lokale Instanz mithilfe der Option -Force auf gemountet ändern.
  - Wenn keine Instanz geöffnet ist, können Sie die lokale Instanz durch Verwenden der Option -Force auf Öffnen ändern.

- **-halten Sie { - stündlich - jeden Tag — monatlich - unbegrenzt}**

  Gibt an, ob das Backup stündlich, täglich, wöchentlich, monatlich oder unbegrenzt aufbewahrt werden soll. Wenn die Option -Retention nicht angegeben ist, wird die Aufbewahrungsklasse standardmäßig auf -hourly gesetzt. Mit der Option -unlimited können Sie Backups für immer aufbewahren. Die Option -unlimited macht das Backup nicht zur Löschung durch die Aufbewahrungsrichtlinie.

- **-Archivprotokolle**

  Gibt die Erstellung eines Backup-Protokolls für das Archivprotokoll an.

- **-Backup-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll für die Sicherung des Archivprotokolls an.

- **-exclude-dest path1, [, [path2]]**

  Gibt die Ziele für das Archivprotokoll an, die vom Backup ausgeschlossen werden sollen.

- *-prunelogs {-all} -bis-scnbis-scn - bis-dateyyyyy-MM-dd:HH:mm:ss - vor {-Monaten

  Gibt an, ob die Archivprotokolldateien aus den Speicherprotokollzielen gelöscht werden sollen, basierend auf den beim Erstellen eines Backups bereitgestellten Optionen. Die Option -all löscht alle Archivprotokolldateien aus den Archivprotokollzielen. Mit der Option -bis-scn werden die Archivprotokolldateien bis zu einer angegebenen Systemändernummer (SCN) gelöscht. Mit der Option -bis -date werden die Archivprotokolldateien bis zum angegebenen Zeitraum gelöscht. Die Option -before löscht die Archivprotokolldateien vor dem angegebenen Zeitraum (Tage, Monate, Wochen, Stunden).

- **-Schedule-Name schedule_Name**

Gibt den Namen an, den Sie für den Zeitplan angeben.

- **-schedule-comment schedule_comment**

  Gibt einen optionalen Kommentar an, um die Planung des Backups zu beschreiben.

- **-Intervall { -stündlich} -täglich / -wöchentlich / -ontimeonly**

  Gibt das Zeitintervall an, mit dem die Backups erstellt werden. Sie können das Backup stündlich, täglich, wöchentlich, monatlich oder einmalig planen.

- **-cronstring cron_string**

  Gibt die Planung des Backups mithilfe von cronstring an. Cron-Ausdrücke werden verwendet, um Instanzen von CronTrigger zu konfigurieren. Cron-Ausdrücke sind Zeichenfolgen, die aus den folgenden Unterausdrücken bestehen:

  - 1 bezieht sich auf Sekunden.
  - 2 bezieht sich auf Minuten.
  - 3 bezieht sich auf Stunden.
  - 4 bezieht sich auf einen Tag im Monat.
  - 5 bezieht sich auf den Monat.
  - 6 bezieht sich auf einen Tag in einer Woche.
  - 7 bezieht sich auf das Jahr (optional).

- **-Startzeit yyyy-MM-dd HH:mm**

  Gibt die Startzeit des geplanten Vorgangs an. Die Startzeit des Zeitplans sollte im Format yyyy-MM-dd HH:mm enthalten sein.

- **-runasuser runasuser**

  Gibt an, dass der Benutzer (Root-Benutzer oder Oracle-Benutzer) des geplanten Backup-Vorgangs während der Planung des Backups geändert wird.

- **-taskSpec taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation an, die für die Vorverarbeitung oder Nachverarbeitung des Backup-Vorgangs verwendet werden kann. Der vollständige Pfad der XML-Datei muss mit der Option -taskSpec bereitgestellt werden.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Der Befehl smo schedule delete

Durch diesen Befehl wird ein Backup-Zeitplan gelöscht, wenn er nicht mehr benötigt wird.

Syntax

```
        smo schedule delete
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die Sie einen Backup-Zeitplan löschen möchten. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Planungsnamen an, den Sie beim Erstellen eines Backup-Zeitplans angegeben haben.

Der Befehl smo schedule list

Mit diesem Befehl werden die geplanten Vorgänge aufgelistet, die einem Profil zugeordnet sind.

Syntax

```
        smo schedule list
-profile profile_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils für die Datenbank an, mit dem Sie eine Liste geplanter Vorgänge anzeigen können. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

Der Smo Schedule Resume Befehl

Mit diesem Befehl wird der ausgesetzt gesperrte Backup-Zeitplan fortgesetzt.

Syntax

```
        smo schedule resume
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die den unterbrochenen Backup-Zeitplan fortsetzen soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Planungsnamen an, den Sie beim Erstellen eines Backup-Zeitplans angegeben haben.

Der Befehl smoplan suspendieren

Mit diesem Befehl wird ein Backup-Zeitplan so lange unterbrochen, bis der Backup-Zeitplan wieder aufgenommen wird.

Syntax

```
        smo schedule suspend
-profile profile_name
-schedule-name schedule_name
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die einen Backup-Zeitplan aussetzen soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Planungsnamen an, den Sie beim Erstellen eines Backup-Zeitplans angegeben haben.

Der Befehl smo schedule Update

Mit diesem Befehl wird der Zeitplan für ein Backup aktualisiert.

Syntax

```
        smo schedule update
-profile profile_name
-schedule-name schedule_name
\[-schedule-comment schedule_comment\]
-interval \{-hourly \| -daily \| -weekly \| -monthly \| -onetimeonly\}
-cronstring cron_string
-start-time \{start_time <yyyy-MM-dd HH:mm\>\}
-runasuser runasuser
\[-taskspec taskspec\]
-force
\[-quiet \| -verbose\]
```

Parameter

- **-profile Profile_Name**

  Gibt den Namen des Profils an, das mit der Datenbank verknüpft ist, die die Sicherung planen soll. Das Profil enthält die Kennung der Datenbank und andere Datenbankinformationen.

- **-Schedule-Name schedule_Name**

  Gibt den Namen an, den Sie für den Zeitplan angeben.

- **-schedule-comment schedule_comment**

  Gibt einen optionalen Kommentar an, um die Planung des Backups zu beschreiben.

- **-Intervall { -stündlich} -täglich / -wöchentlich / -ontimeonly**

  Gibt das Zeitintervall an, mit dem die Backups erstellt werden. Sie können das Backup nur stündlich, täglich, wöchentlich, monatlich oder einmalig planen.

- **-cronstring cron_string**

  Gibt an, das Backup mit cronstring zu planen. Cron-Ausdrücke werden verwendet, um Instanzen von CronTrigger zu konfigurieren. Cron-Ausdrücke sind Zeichenfolgen, die tatsächlich aus sieben Unterausdrücken bestehen:

  - 1 bezieht sich auf Sekunden
  - 2 bezieht sich auf Minuten
  - 3 bezieht sich auf Stunden
  - 4 bezieht sich auf einen Tag im Monat
  - 5 bezieht sich auf den Monat
  - 6 bezieht sich auf einen Tag in einer Woche
  - 7 bezieht sich auf das Jahr (optional)

- **-Startzeit yyyy-MM-dd HH:mm**

  Gibt die Startzeit des Zeitplanvorgangs an. Die Startzeit des Zeitplans sollte im Format yyyy-MM-dd

HH:mm enthalten sein.

- **-runasuser runasuser**

  Gibt an, den Benutzer des geplanten Backup-Vorgangs während der Planung des Backups zu ändern.

- **-taskSpec taskSpec**

  Gibt die XML-Datei für die Aufgabenspezifikation an, die für die Vorverarbeitung oder Nachverarbeitung des Backup-Vorgangs verwendet werden kann. Der vollständige Pfad der XML-Datei sollte zur Verfügung gestellt werden, die die Option -taskSpec geben.

Der Befehl smo Storage list

Sie können den Befehl Storage list ausführen, um die Liste der Speichersysteme anzuzeigen, die einem bestimmten Profil zugeordnet sind.

Syntax

```
        smo storage list
-profile profile
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Der Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

Beispiel

Im folgenden Beispiel werden die Speichersysteme angezeigt, die dem Profil mjullian zugeordnet sind:

```
smo storage list -profile mjullian
```

```
Sample Output:
Storage Controllers
--------------------
FAS3020-RTP07OLD
```

Der Befehl smo Storage umbenennen

Dieser Befehl aktualisiert den Namen oder die IP-Adresse des Speichersystems.

Syntax

```
        smo storage rename
-profile profile
-oldname old_storage_name
-newname new_storage_name
\[-quiet \| -verbose\]
```

Parameter

- **-Profil**

  Gibt den Namen des Profils an. Dieser Name kann bis zu 30 Zeichen lang sein und muss innerhalb des Hosts eindeutig sein.

- **-oldname old_Storage_Name**

  Gibt die IP-Adresse oder den Namen des Storage-Systems an, bevor das Storage-System umbenannt wird. Sie müssen die IP-Adresse oder den Namen des Speichersystems eingeben, die angezeigt wird, wenn Sie den Befehl smoStorage list ausführen.

- **-newname New_Storage_Name**

  Gibt die IP-Adresse oder den Namen des Storage-Systems nach der Umbenennung des Storage-Systems an.

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel

Im folgenden Beispiel wird der Befehl smo Storage umbenennen, um das Speichersystem umzubenennen:

```
smo storage rename -profile mjullian -oldname lech -newname hudson
-verbose
```

Der SMO System Dump Befehl

Sie können den Systemdump-Befehl ausführen, um eine JAR-Datei zu erstellen, die Diagnoseinformationen zur Serverumgebung enthält.

Syntax

```
        smo system dump
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel des Befehls „System Dump“

Im folgenden Beispiel wird der Befehl smo System dump verwendet, um eine JAR-Datei zu erstellen:

```
smo system dump
Path: C:\\userhomedirectory\\netapp\\smo\\3.3.0\\smo_dump_hostname.jar
```

Der Befehl smo System verify

Dieser Befehl bestätigt, dass alle Komponenten der Umgebung, die zum Ausführen von SnapManager erforderlich sind, ordnungsgemäß eingerichtet werden.

Syntax

```
        smo system verify
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen auf der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt Fehler-, Warn- und Informationsmeldungen an der Konsole an.

Beispiel des Befehls „System verify“

Im folgenden Beispiel wird der Befehl smo System verify verwendet.

```
smo system verify
SMO-13505 [INFO ]: Snapdrive verify passed.
SMO-13037 [INFO ]: Successfully completed operation: System Verify
SMO-13049 [INFO ]: Elapsed Time: 0:00:00.559
Operation Id [N4f4e910004b36cfecee74c710de02e44] succeeded.
```

Der Befehl smo Version

Sie können den Versionsbefehl ausführen, um festzulegen, welche Version von SnapManager Sie auf Ihrem lokalen Host ausführen.

Syntax

```
        smo version
\[-quiet \| -verbose\]
```

Parameter

- **-ruhig**

  Zeigt nur Fehlermeldungen in der Konsole an. Standardmäßig werden Fehler- und Warnmeldungen angezeigt.

- **-verbose**

  Zeigt das Erstellungsdatum und den Inhalt der einzelnen Profile an. Zeigt auch Fehler-, Warn- und Informationsmeldungen in der Konsole an.

Beispiel des Versionsbefehls

Im folgenden Beispiel wird die Version des SnapManager angezeigt:

```
smo version
SnapManager for Oracle Version: 3.3.1
```

SnapManager zur Fehlerbehebung

Hier finden Sie Informationen über einige der häufigsten Probleme, die auftreten können, und über deren Behebung.

In der folgenden Tabelle werden häufige Probleme und mögliche Lösungen beschrieben:

Frage, die nur mit Problemen zu tun hat	Mögliche Lösung

Werden die Zieldatenbank und der Listener ausgeführt?	Führen Sie den Befehl lsnrctl Status aus. Stellen Sie sicher, dass die Datenbankinstanz beim Listener registriert ist.
Ist der Storage sichtbar?	Führen Sie folgende Schritte aus: 1. Klicken Sie mit der rechten Maustaste auf Arbeitsplatz, und wählen Sie dann **Verwalten**. 2. Klicken Sie auf **Storage** > **SnapDrive** > **Hostname** > **Festplatten**.
Wird der SnapManager Server ausgeführt?	Überprüfen Sie den Status, und starten Sie den Server mithilfe der Servicekonfiguration. Bevor Sie SnapManager-Befehle für Profile mit der grafischen Benutzeroberfläche (GUI) oder der Befehlszeilenschnittstelle (CLI) initiieren können, muss der Server ausgeführt werden. Sie können Repositorys erstellen oder aktualisieren, ohne den Server zu starten. Um jedoch alle anderen SnapManager-Vorgänge auszuführen, muss der Server ausgeführt werden. Geben Sie zum Starten des SnapManager-Servers den folgenden Befehl ein: smo_Server starte.
Sind alle Komponenten erforderlich, um SnapManager korrekt auszuführen?	Führen Sie den smo System verify Befehl aus, um zu überprüfen, dass SnapDrive korrekt eingerichtet ist.
Verfügen Sie über die richtige Version von SnapManager?	Verwenden Sie den Befehl smo Version, um die SnapManager-Version zu überprüfen.

Haben Sie sich die Protokolldateien von SnapManager angesehen, um zu ermitteln, ob die Fehlermeldungen helfen können, das Problem zu isolieren?	SnapManager zeichnet alle Log-Einträge in einem Satz rotierender Log-Dateien auf. Die Log-Dateien sind unter C:\Program_Files\NetApp\SnapManager für Oracle\logs zu finden. Wenn Sie Windows 2008 verwenden, befinden sich die Protokolle an folgenden Orten: • Betriebsprotokolle: ◦ C:\Programme\NetApp\SnapManager für Oracle\var\log\smo • Client-Protokolle: ◦ C:\Users\Administrator\AppData\Roaming\NetApp\smo\3.3.0\ Es könnte auch hilfreich sein, sich die Protokolle an folgender Stelle anzusehen: C:\Dokumente und Einstellungen\Hostname\Applikationsdaten\NetApp\smo\3.3.0\log Jedes Betriebsprotokoll wird in seine eigene Protokolldatei der Form smo_of_date_time.log geschrieben.
Wenn auf einem Storage-System, auf dem Data ONTAP nicht ausgeführt wird, Archivprotokolle gespeichert sind, haben Sie diese von Überlegungen für Backups mit SnapManager ausgeschlossen?	Mit der Datei smo.config können Sie bestimmte Archiv-Log-Dateien ausschließen. Für Windows befindet sich die Datei an der folgenden Stelle: C:\Program_Files\NetApp\smo\Properties\smo.config Verwenden Sie das in der Datei erwähnte Format, um die lokalen Archivprotokolle auszuschließen. Weitere Informationen finden Sie im Thema „SBenetzungskonfigurationseigenschaften“. Sie können die Ziele für das Archivprotokoll auch ausschließen, wenn Sie ein Backup von der SnapManager-CLI erstellen. Weitere Informationen finden Sie im Thema „Datenbanksicherungen erstellen“. Sie können die Ziele für das Archivprotokoll auch ausschließen, wenn Sie ein Backup von der SnapManager-GUI erstellen.

Haben Sie ein MS-DOS-Fenster in dem Verzeichnis, in dem Sie versuchen, SnapManager unter Windows zu installieren oder zu aktualisieren?	Es wird eine Fehlermeldung wie die folgende angezeigt: `Directory C:\Program Files\NetApp\SnapManager for Oracle\bin is currently in use by another program.` Alle Fenster, die von Ihnen oder einem anderen Benutzer geöffnet werden, die derzeit auf dieses Verzeichnis verweisen, müssen geschlossen werden, bevor die Installation fortgesetzt werden kann. Schließen Sie das Fenster, und versuchen Sie die Installation oder führen Sie ein Upgrade erneut durch.
Konnte keine Verbindung zum Repository hergestellt werden?	Wenn die Verbindung zu einem Repository fehlschlägt, führen Sie den Befehl lsnrctl Status in der Repository-Datenbank aus, und überprüfen Sie die aktiven Dienstnamen. Wenn SnapManager eine Verbindung zur Repository-Datenbank herstellt, wird der Servicename der Datenbank verwendet. Je nach Einrichtung des Listeners kann dies der kurze Servicename oder der vollqualifizierte Servicename sein. Wenn SnapManager eine Verbindung zu einer Datenbank für einen Backup-, Restore- oder anderen Vorgang herstellt, verwendet er den Host-Namen und den SID. Wenn das Repository nicht korrekt initialisiert wird, weil es derzeit nicht erreichbar ist, erhalten Sie eine Fehlermeldung, in der Sie gefragt werden, ob Sie das Repository entfernen möchten. Sie können das Repository aus Ihrer aktuellen Ansicht entfernen, sodass Sie Vorgänge für andere Repositories ausführen können. Prüfen Sie außerdem, ob der entsprechende Service ausgeführt wird.
Kann das System den Hostnamen auflösen?	Überprüfen Sie, ob sich der angegebene Hostname in einem anderen Subnetz befindet. Wenn Sie eine Fehlermeldung erhalten, dass SnapManager den Hostnamen nicht auflösen kann, fügen Sie den Hostnamen in die Hostdatei hinzu. Fügen Sie den Hostnamen zur Datei hinzu, die sich unter C:\WINDOWS\system32\drivers\etc\Hosts befindet: Xxx.xxx.xxx.xxx Hostname IP-Adresse
Führt SnapDrive aus?	Um den Status von SnapDrive anzuzeigen, gehen Sie zu Dienste, und wählen Sie dann den SnapDrive-Dienst aus.

Welche Storage-Systeme sind für den Zugriff mit SnapDrive konfiguriert?	So suchen Sie die für SnapDrive konfigurierten Storage-Systeme: 1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie dann **Verwalten**. 2. Klicken Sie auf **Storage** > **SnapDrive**. 3. Klicken Sie mit der rechten Maustaste auf den Hostnamen und wählen Sie dann **Transportprotokoll-Einstellungen** aus.

Wie kann die SnapManager GUI Performance verbessert werden?	• Stellen Sie sicher, dass Sie über gültige Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil verfügen. Wenn Ihre Anmeldedaten ungültig sind, löschen Sie die Benutzeranmeldeinformationen für das Repository, den Profilhost und das Profil. Setzen Sie dieselben Benutzeranmeldeinformationen zurück, die Sie zuvor für das Repository, den Profilhost und das Profil festgelegt haben. Weitere Informationen zum erneuten Einstellen der Benutzeranmeldeinformationen finden Sie unter „`SFestlegen von Anmeldeinformationen nach Löschen des Anmeldeinformationscache`“. • Schließen Sie die nicht verwendeten Profile. Wenn mehr Profile geöffnet werden, wird die Performance der SnapManager GUI beeinträchtigt. • Überprüfen Sie, ob Sie **beim Start öffnen** im Fenster Benutzereinstellungen im Menü **Admin** in der SnapManager-Benutzeroberfläche aktiviert haben. Wenn dies aktiviert ist, wird die unter C:\Dokumente und Einstellungen\Administrator\Anwendungsdaten\NetApp\smo\3.3.0\gui\Status verfügbare Benutzerkonfigurationsdatei (user.config) als openOnStartup=PROFIL angezeigt. Da **Öffnen auf Start** aktiviert ist, müssen Sie nach kürzlich geöffneten Profilen aus der SnapManager-Benutzeroberfläche suchen, wobei lastOpenProfiles in der Benutzerkonfiguration (user.config)-Datei verwendet werden: LASTOPENPROFILE1,PROFILE2,PROFIL3,… Sie können die aufgeführten Profilnamen löschen und immer eine minimale Anzahl von Profilen als offen halten. • Löschen Sie vor der Installation der neuen Version von SnapManager in der Windows-basierten Umgebung die clientseitigen Einträge von SnapManager, die an folgender Stelle verfügbar sind: C:\Dokumente und Einstellungen\Administrator\Applikationsdaten\NetApp

Wenn mehrere SnapManager Vorgänge gestartet und gleichzeitig im Hintergrund ausgeführt werden, benötigt die SnapManager GUI mehr Zeit für die Aktualisierung. Wenn Sie mit der rechten Maustaste auf das Backup klicken (das bereits gelöscht ist, aber immer noch in der SnapManager GUI angezeigt wird), sind die Backup-Optionen für dieses Backup nicht im Fenster Backup oder Clone aktiviert.	Sie müssen warten, bis die SnapManager GUI aktualisiert wird, und dann den Backup-Status überprüfen.
Was würden Sie tun, wenn die Oracle-Datenbank nicht auf Englisch eingestellt ist?	SnapManager-Vorgänge können fehlschlagen, wenn die Sprache für eine Oracle-Datenbank nicht auf Englisch gesetzt ist.die Sprache der Oracle-Datenbank auf Englisch setzen: 1. Stellen Sie sicher, dass die Umgebungsvariable NLS_LANG nicht eingestellt ist: Echo%NLS_LANG% 2. Fügen Sie die folgende Zeile der Datei Wrapper.conf hinzu: C:\SnapManager_install_Directory\Service: Set.NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252 3. Starten Sie den SnapManager-Server neu: smo_Server wird neu gestartet Wenn die Umgebungsvariable des Systems auf NLS_LANG gesetzt ist, müssen Sie das Skript bearbeiten, um NLS_LANG nicht zu überschreiben.

Was würden Sie tun, wenn die Backup-Planung fehlschlägt, wenn die Repository-Datenbank auf mehr als eine IP verweist und jede IP einen anderen Hostnamen hat?	1. Beenden Sie den SnapManager-Server. 2. Löschen Sie die Zeitplandateien im Repository-Verzeichnis von den Hosts, auf denen Sie den Backup-Zeitplan auslösen möchten. Die Namen der Zeitplandateien können in den folgenden Formaten vorliegen: ◦ Repository#repo_username#Repository_Database_Name#Repository_Host#repo_Port ◦ Repository-repo_usernamerepository_Database_Name-Repository_Host-repo_Port **Hinweis:** Sie müssen sicherstellen, dass Sie die Terminplandatei in dem Format löschen, das den Details des Projektarchivs entspricht. 3. Starten Sie den SnapManager-Server neu. 4. Öffnen Sie andere Profile unter dem gleichen Repository von der SnapManager GUI, um sicherzustellen, dass keine Terminplaninformationen dieser Profile fehlen.
Was würden Sie tun, wenn der SnapManager-Vorgang mit dem Fehler der Dateisperre für Zugangsdaten fehlschlägt?	SnapManager sperrt die Anmeldeinformationsdatei vor dem Aktualisieren und entsperrt sie nach dem Aktualisieren.Wenn mehrere Operationen gleichzeitig ausgeführt werden, kann einer der Operationen die Anmeldeinformationsdatei sperren, um sie zu aktualisieren. Wenn ein anderer Vorgang versucht, gleichzeitig auf die Datei mit gesperrten Anmeldeinformationen zuzugreifen, schlägt der Vorgang mit dem Dateisperrfehler fehl. Konfigurieren Sie in der Datei smo.config die folgenden Parameter, je nach Häufigkeit der gleichzeitigen Operationen: • FileLock.retryIntervall = 100 Millisekunden • FileLock.Timeout = 5000 Millisekunden Die den Parametern zugewiesenen Werte müssen in Millisekunden liegen.

Was würden Sie tun, wenn der Zwischenstatus des Backup Verify-Vorgangs auf der Registerkarte Monitor fehlgeschlagen angezeigt wird, obwohl der Backup Verify-Vorgang noch ausgeführt wird?	Die Fehlermeldung wird in der Datei sm_gui.log protokolliert. Sie müssen in der Protokolldatei nachsehen, um die neuen Werte für den Vorgang zu bestimmen.heartbeatIntervall und Operation.heartbeatThreshold Parameter, die dieses Problem lösen werden. 1. Fügen Sie die folgenden Parameter in der Datei smo.config hinzu: ◦ Operation.heartbeatIntervall = 5000 ◦ Operation.heartbeatThreshold = 5000 der von SnapManager zugewiesene Standardwert ist 5000. 2. Diesen Parametern die neuen Werte zuweisen. Die den Parametern zugewiesenen Werte müssen in Millisekunden liegen. 3. Starten Sie den SnapManager-Server neu, und führen Sie den Vorgang erneut aus.
Was ist zu tun, wenn ein Heap-Space-Problem auftritt?	Wenn während des SnapManager für Oracle-Betriebs ein Heap-Space-Problem auftritt, müssen Sie die folgenden Schritte durchführen: 1. Wechseln Sie zum Installationsverzeichnis für SnapManager für Oracle. 2. Öffnen Sie die Datei launchjava aus dem Installationsverzeichnis\bin\launchjava Pfad. 3. Erhöhen Sie den Wert des Java -Xmx160m Java Heap-space Parameters. So können Sie beispielsweise den Standardwert von 160 m auf 200 m erhöhen. Wenn Sie den Wert des Java Heap-space-Parameters in den früheren Versionen von SnapManager für Oracle erhöht haben, sollten Sie diesen Wert beibehalten.

Was würden Sie tun, wenn die SnapManager-Dienste nicht in einer Windows-Umgebung starten und die folgende Fehlermeldung angezeigt wird: Windows konnte den Snap-Manager auf dem lokalen Computer nicht starten. Weitere Informationen finden Sie im Systemereignisprotokoll. Wenn es sich um einen nicht-Microsoft-Dienst handelt, wenden Sie sich an den Serviceanbieter, und wenden Sie sich an den dienstspezifischen Fehlercode 1?	Konfigurieren Sie die folgenden Parameter in der Datei wrapper.conf, die sich im Dienst Installation_Directory\befindet. • Der Parameter Wrapper Startup Timeout definiert die maximal zulässige Zeit zwischen dem Wrapper, der die Java Virtual Machine (JVM) startet, und der Antwort von der JVM, die die Anwendung gestartet hat. Der Standardwert ist 90 Sekunden. Sie können jedoch einen Wert größer als 0 ändern. Wenn Sie einen ungültigen Wert angeben, wird stattdessen die Standardeinstellung verwendet. • Der Parameter wrapper.ping.Timeout definiert die maximal zulässige Zeit zwischen dem Wrapper, der die JVM anpingen soll, und der Antwort von JVM. Der Standardwert ist 90 Sekunden. Sie können jedoch in einen Wert größer 0 ändern. Wenn Sie einen ungültigen Wert angeben, wird stattdessen die Standardeinstellung verwendet.

Speicherauszug-Dateien

Die Dump-Dateien sind komprimierte Log-Dateien, die Informationen über SnapManager und seine Umgebung enthalten. Die verschiedenen Typen von erstellten Log-Dateien sind Operation, Profil und System-Dump-Datei.

Sie können den Dump-Befehl oder die Registerkarte **Create Diagnostics** in der grafischen Benutzeroberfläche (GUI) verwenden, um Informationen über einen Vorgang, ein Profil oder die Umgebung zu sammeln. Ein System-Dump erfordert kein Profil. Das Profil und die Operation Dumps erfordern jedoch Profile.

SnapManager enthält die folgenden Diagnoseinformationen in der Dump-Datei:

- Die durchgeführten Schritte
- Die Zeitdauer für jeden Schritt
- Das Ergebnis jedes Schritts
- Fehler, falls vorhanden, der während des Vorgangs aufgetreten ist

SnapManager-Protokolldateien oder Dump-Dateien ermöglichen Lese- und Schreibberechtigungen nur für die Root-Benutzer und die anderen Benutzer, die zur Root-Benutzergruppe gehören.

SnapManager enthält auch die folgenden Informationen in der Datei:

- Version und Architektur des Betriebssystems
- Umgebungsvariablen

- Java-Version
- SnapManager Version und Architektur
- SnapManager-Einstellungen
- SnapManager Nachrichten
- Eigenschaften log4j
- SnapDrive Version und Architektur
- SnapDrive-Protokolldateien
- Oracle Version
- Oracle Owatch – Details zum lokalen Bestand
- Oracle Version der Repository-Datenbank
- Typ der Zieldatenbank (eigenständig)
- Zieldatenbankrolle (primärer, physischer Standby oder logischer Standby)
- Einrichtung der Zieldatenbank Oracle Recovery Manager (RMAN) (keine RMAN Integration, RMAN mit Kontrolldateien oder RMAN mit Katalogdatei)
- Oracle Version der Zieldatenbank
- System Identifier (SID) der Zieldatenbank
- RMAN-Datenbankname und TNS-Verbindungsname
- Name des Repository-Datenbankdienstes
- Auf dem Host installierte Datenbankinstanzen
- Profildeskriptor
- Maximaler gemeinsam genutzter Speicher
- Swap-Informationen zum Speicherplatz
- Speicherinformationen
- Multipath-Umgebung
- Host Utilities-Version
- Microsoft Internet Small Computer System Interface (iSCSI) Software Initiator-Version für Windows
- Ausgabe des Befehls „System Verify“

In der Dump-Datei werden auch die SnapManager-Einschränkungen unter Windows aufgeführt.

SnapManager Dump-Dateien enthalten auch die SnapDrive Datensammler-Datei und die Oracle Alert Log-Datei. Sie können die Oracle Alert Log-Datei unter Verwendung der SMO Operation Dump und smo profile dump Befehle sammeln.

System Dump enthält keine Oracle-Alarmprotokolle. Das Profil und die Operation Dumps enthalten jedoch die Alarmprotokolle.

Selbst wenn der SnapManager Host Server nicht ausgeführt wird, können Sie über die Befehlszeilenschnittstelle (CLI) oder die GUI auf die Dump-Informationen zugreifen.

Wenn ein Problem auftritt, das nicht gelöst werden kann, können Sie diese Dateien an NetApp Global Services senden.

Erstellen von Dump-Dateien auf Betriebsebene

Sie können den Befehl smo Operation dump mit dem Namen oder der ID des fehlgeschlagenen Vorgangs verwenden, um Protokollinformationen über einen bestimmten Vorgang zu erhalten. Sie können unterschiedliche Protokollebenen festlegen, um Informationen zu einem bestimmten Vorgang, Profil, Host oder einer bestimmten Umgebung zu erfassen.

1. Geben Sie den folgenden Befehl ein:Smo Operation dump -idguid

   Der smo Operation dump Befehl stellt einen super Satz der Informationen zur Verfügung, die vom smo profile dump Befehl bereitgestellt werden, was wiederum einen super Satz von den Informationen bietet, die vom smo System dump Befehl zur Verfügung gestellt werden.

   Speicherverzeichnis der Speicherdatei:

   ```
   Path:\<user-home>\Application
   Data\NetApp\smo\3.3.0\smo_dump_8abc01c814649ebd0114649ec69d0001.jar
   ```

Erstellen von Dump-Dateien auf Profilebene

Mithilfe des Befehls smo profile dump mit dem Namen des Profils können Sie Protokollinformationen zu einem bestimmten Profil finden.

1. Geben Sie den folgenden Befehl ein: smo profile dump -profile Profile_Name

   Speicherverzeichnis der Speicherdatei:

   ```
   Path:\<user-home>\Application
   Data\NetApp\smo\3.3.0\smo_dump_8abc01c814649ebd0114649ec69d0001.jar
   ```

   Wenn beim Erstellen eines Profils ein Fehler auftritt, verwenden Sie den Befehl „Smosystem dump“. Nachdem Sie ein Profil erfolgreich erstellt haben, verwenden Sie die Befehle SmoOperation dump und scoprofile dump.

Erstellen von Dump-Dateien auf Systemebene

Sie können den smo System Dump Befehl verwenden, um Protokollinformationen über den SnapManager Host und die Umgebung zu erhalten. Sie können unterschiedliche Protokollebenen angeben, um Informationen zu einem bestimmten Vorgang, Profil oder Host und Umgebung zu erfassen.

1. Geben Sie den folgenden Befehl ein: smo System Dump

   Daraus resultierender Dump

```
Path:\<user-home>\Application
Data\NetApp\smo\3.3.0\smo_dump_server_host.jar
```

So finden Sie Speicherauszugsdateien

Die Dump-Datei befindet sich im Client-System für einfachen Zugriff. Diese Dateien sind hilfreich, wenn Sie Probleme im Zusammenhang mit Profil, System oder einer beliebigen Operation beheben müssen.

Die Dump-Datei befindet sich im Home-Verzeichnis des Benutzers auf dem Client-System.

- Wenn Sie die grafische Benutzeroberfläche (GUI) verwenden, befindet sich die Dump-Datei unter:

```
user_home\Application Data\NetApp\smo\3.3.0\smo_dump dump_file_type_name
server_host.jar
```

- Wenn Sie die Befehlszeilenschnittstelle (CLI) verwenden, befindet sich die Dump-Datei unter:

```
user_home\.netapp\smo\3.3.0\smo_dump_dump_file_type_name server_host.jar
```

Die Dump-Datei enthält die Ausgabe des Dump-Befehls. Der Name der Datei hängt von den angegebenen Informationen ab. In der folgenden Tabelle werden die Typen von Dump-Operationen und die daraus resultierenden Dateinamen angezeigt:

Typ des Speicherauszugsvorgangs	Dateiname wird angezeigt
Befehl für den Operation Dump mit Vorgangs-ID	smo_dump_operation-id.jar

Der Befehl für den Operation Dump enthält keine Vorgangs-ID	smo Operation Dump -Profile VH1-verbose die folgende Ausgabe wird angezeigt:
	`smo operation dump -profile VH1 -verbose`
	`[ INFO] SMO-13048: Dump Operation Status: SUCCESS`
	`[ INFO] SMO-13049: Elapsed Time: 0:00:01.404`
	`Dump file created.`
	`Path: user_home\Application Data\ontap\smo\3.3.0\smo_dump_VH1_kaw.rtp.foo.com.jar`

Befehl für System Dump	smo_dump_host-name.jar
Profildump-Befehl	smo_dump_profile-name_host-name.jar

So sammeln Sie Speicherauszugsdateien

Sie können -dump in den SnapManager-Befehl einschließen, um die Dump-Dateien nach einem erfolgreichen oder fehlgeschlagenen SnapManager-Vorgang zu sammeln.

Sie können Dump-Dateien für die folgenden SnapManager-Vorgänge sammeln:

- Profile werden erstellt
- Profile werden aktualisiert
- Backups werden erstellt
- Backups werden überprüft
- Backups werden gelöscht
- So werden Backups entlastet
- Montage von Backups
- UnMounten von Backups
- Backups werden wiederhergestellt
- Klone werden erstellt
- Klone werden gelöscht

Wenn Sie ein Profil erstellen, können Sie Dump-Dateien nur sammeln, wenn der Vorgang erfolgreich ist. Wenn beim Erstellen eines Profils ein Fehler auftritt, müssen Sie den Befehl „Smosystem dump“ verwenden. Für erfolgreiche Profile können Sie die SmoOperation Dump und smoprofile Dump-Befehle verwenden, um die Dump-Dateien zu sammeln.

Beispiel

```
      smo  backup create -profile targetdb1_prof1 -auto -full -online
-dump
```

Sammeln zusätzlicher Protokollinformationen für eine einfachere Fehlersuche

Wenn Sie zusätzliche Protokolle benötigen, um einen fehlgeschlagenen SnapManager-Vorgang zu debuggen, müssen Sie eine externe Umgebungsvariable Server.log.Level festlegen. Diese Variable überschreibt die Standard-Protokollebene und lädt alle Protokollmeldungen in der Protokolldatei ab. Sie können beispielsweise die Protokollebene in DEBUG ändern, die zusätzliche Meldungen protokolliert und beim Debuggen von Problemen helfen kann.

Die SnapManager-Protokolle sind an folgenden Orten zu finden:

- SnapManager_install_Directory\log

Um die Standard-Protokollebene außer Kraft zu setzen, müssen Sie die folgenden Schritte durchführen:

1. Erstellen Sie eine Platform.override-Textdatei im SnapManager-Installationsverzeichnis.
2. Fügen Sie den Parameter Server.log.Level in die Textdatei Platform.override ein.
3. Weisen Sie einen Wert zu (TRACE, DEBUG, INFO, WARN, ERROR, FATAL oder PROGRESS) zum Parameter Server.log.Level.

   Um z. B. die Protokollebene auf FEHLER zu ändern, setzen Sie den Wert von Server.log.Level auf FEHLER.

   Server.log.Level=FEHLER

4. Starten Sie den SnapManager-Server neu.

Wenn keine zusätzlichen Protokollinformationen erforderlich sind, können Sie den Parameter Server.log.Level aus der Textdatei Platform.override löschen.

SnapManager verwaltet die Menge der Server-Log-Dateien auf der Grundlage der benutzerdefinierten Werte der folgenden Parameter in der Datei smo.config:

- Log.max_log_files
- Log.max_log_file_size
- Log.max_Rolling_Operation_Factory_logs

Fehlerbehebung bei Klonproblemen

Hier finden Sie Informationen darüber, die während eines Klonens auftreten können und wie Sie sie lösen können.

Symptom	Erklärung	Behelfslösung
Der Klonvorgang schlägt fehl, wenn das Archivziel auf USE_DB_RECOVERY_FILE_DEST gesetzt ist.	Wenn sich das Archivziel auf USE_DB_RECOVERY_FILE_DEST bezieht, verwaltet der Flash Recovery Area (FRA) aktiv das Archivprotokoll. SnapManager nutzt den FRA-Standort nicht während Klon- oder Restore-Vorgängen und schlägt somit fehl.	Ändern Sie das Archivziel in den tatsächlichen Speicherort des Archivprotokolls anstelle des FRA-Speicherorts.

Der Klonvorgang schlägt mit der folgenden Fehlermeldung fehl: Der Vorgang kann nicht ausgeführt werden: Clone Create. Ursache: ORACLE-00001: Fehler beim Ausführen von SQL: [DATENBANK ÄNDERN ÖFFNEN RESETLOGS;]. Der Befehl zurückgegeben: ORA-01195: Online Backup der Datei 1 benötigt mehr Wiederherstellung, um konsistent zu sein.	Dieses Problem tritt auf, wenn Oracle Listener die Verbindung zur Datenbank nicht herstellen kann.	Wenn Sie ein Backup mit der GUI von SnapManager klonen, führen Sie die folgenden Aktionen durch: 1. Klicken Sie im Repository-Baum auf **Repository** > **Host** > **Profil**, um die Backups anzuzeigen. 2. Klicken Sie mit der rechten Maustaste auf das Backup, das Sie klonen möchten, und wählen Sie **Clone** aus. 3. Geben Sie auf der Seite Clone Initialization die obligatorischen Werte ein, und wählen Sie die Methode Clone Specification aus. 4. Wählen Sie auf der Seite „Spezifikation klonen“ die Option **Parameter** aus. 5. Klicken Sie auf die Registerkarte **+Parameter**. 6. Geben Sie im Feld **Parametername** den Namen als local_Listener ein und klicken Sie auf **OK**. 7. Aktivieren Sie das Kontrollkästchen **Standard überschreiben** für die Zeile Local_Listener. 8. Klicken Sie auf einen beliebigen Parameter, doppelklicken Sie dann auf den Parameter Local_Listener, und geben Sie den folgenden Wert ein:(ADDRESS=(PROTOCOL=TCP)(HOST=<your_Host_Name>)(PORT=<Port#>)) 9. Klicken Sie Auf **In Datei Speichern**. 10. Klicken Sie auf **Weiter** und fahren Sie mit dem Clone create Wizard fort. Wenn Sie ein Backup über CLI klonen, müssen Sie die folgenden Informationen in das Tag **<Parameter>** der Klon-Spezifikations-Datei einfügen:

Der Klonvorgang schlägt mit einer Fehlermeldung fehl, die sagt, dass der von Ihnen verwendete Mountpoint bereits verwendet ist.	Mit SnapManager können Sie einen Klon nicht über einem bestehenden Bereitstellungspunkt mounten. Ein unvollständiger Klon hat den Bereitstellungspunkt nicht entfernt.	Geben Sie einen anderen Bereitstellungspunkt an, der vom Klon verwendet werden soll, oder heben Sie den problematischen Bereitstellungspunkt auf.
Der Klonvorgang schlägt fehl mit einer Fehlermeldung, dass Datendateien keine .dbf-Erweiterung haben.	Einige Versionen des Oracle NID-Dienstprogramms funktionieren nicht mit Datendateien, es sei denn, die Dateien verwenden eine .dbf-Erweiterung.	• Benennen Sie die Datendatei um, um eine .dbf-Erweiterung zu erhalten. • Wiederholen Sie den Sicherungsvorgang. • Klonen des neuen Backups:
Aufgrund der nicht erfüllten Anforderungen schlägt der Klonvorgang fehl.	Sie versuchen, einen Klon zu erstellen. Einige der Voraussetzungen wurden jedoch nicht erfüllt.	Fahren Sie wie unter *Erstellen eines Klons* beschrieben fort, um die Voraussetzungen zu erfüllen.
SnapManager für Oracle klont keine physischen Oracle Data Guard Standby Datenbanken (10.2.0.5).	SnapManager für Oracle deaktiviert den verwalteten Recovery-Modus nicht, während ein Offline-Backup der physischen Oracle 10gR2 (10.2.0.5) Standby-Datenbanken durchgeführt wird, die mit Oracle Data Guard Services erstellt wurden. Aufgrund dieses Problems ist das Offline Backup inkonsistent. Wenn SnapManager für Oracle versucht, das Offline-Backup zu klonen, wird nicht einmal versucht, eine Wiederherstellung auf der geklonten Datenbank durchzuführen. Da das Backup inkonsistent ist, muss die geklonte Datenbank wiederhergestellt werden, und damit kann Oracle den Klon nicht erfolgreich erstellen.	Aktualisieren Sie die Oracle-Datenbank auf Oracle 11gR1 (Patch 11.1.0.7).

Fehlerbehebung bei Problemen mit der grafischen Benutzeroberfläche

Sie finden Informationen zu einigen Problemen der grafischen Benutzeroberfläche (GUI), die Ihnen bei der Problembehebung helfen könnten.

Problem	Erklärung	Behelfslösung

Beim Zugriff auf die SnapManager-Benutzeroberfläche zur Durchführung eines Vorgangs kann die folgende Fehlermeldung angezeigt werden: SMO-20111 : Authentifizierung für Benutzer auf dem Host fehlgeschlagen.	Dieses Problem tritt auf, wenn das Kennwort des Benutzers in dem Host geändert wird, auf dem der SnapManager-Server ausgeführt wird.Nachdem das Passwort geändert wurde, wird der Anmeldeinformationscache, der für den Benutzer erstellt wird, der die GUI gestartet hat, ungültig. Die SnapManager-GUI verwendet zur Authentifizierung weiterhin die Zugangsdaten im Cache und schlägt somit fehl.	Sie müssen eine der folgenden Aufgaben durchführen: • Löschen Sie die Anmeldeinformationen des Benutzers, dessen Passwort geändert wurde, und fügen Sie dann die neuen Anmeldeinformationen in den Cache ein, indem Sie die folgenden Befehle ausführen: a. löschen von smo-Anmeldeinformationen b. smo Credentials-Satz • Löschen Sie den gesamten Cache, indem Sie den Befehl smo centimals clear ausführen. Öffnen Sie die GUI erneut, und legen Sie die Anmeldeinformationen fest, falls Sie dazu aufgefordert werden.
Die Sicherheitswarnung wird angezeigt, wenn Sie Java Web Start verwenden, um auf die SnapManager-GUI zuzugreifen.	Beim Zugriff auf die SnapManager-GUI mit Java Web Start wird eine Sicherheitswarnung angezeigt.Dieses Problem tritt auf, weil JNLP-JARs selbstsigniert sind und die von SnapManager verwendete Java-Version keine selbstsignierten Jars auf hoher Sicherheitsstufe zulässt.	Ändern Sie entweder die Sicherheitseinstellungen im java-Bedienfeld auf Medium, oder fügen Sie die SnapManager-GUI-URL zur Ausnahmeliste hinzu.
In der SnapManager Webstart-GUI wird die falsche Version angezeigt.	Nachdem Sie beim Start der Web-Start-GUI die SnapManager von einer neueren Version auf eine frühere Version heruntergestuft haben, wird die neuere Version der SnapManager Web-Start-GUI gestartet.	Sie müssen den Cache auch löschen, indem Sie die folgenden Schritte durchführen: 1. Klicken Sie auf **Start** und wählen Sie **Ausführen**. 2. Geben Sie Folgendes ein: Javaws -Viewer 3. Klicken Sie im Java Cache Viewer-Bildschirm mit der rechten Maustaste auf die SnapManager-Anwendung und wählen Sie **Löschen** aus.

Wenn Sie die GUI neu starten und versuchen, die Backups auf ein bestimmtes Profil zu überprüfen, werden nur die Namen der Profile angezeigt.	SnapManager zeigt erst Informationen zu einem Profil an, wenn Sie es öffnen.	Führen Sie folgende Schritte aus: 1. Klicken Sie mit der rechten Maustaste auf das Profil und wählen Sie im Menü * Öffnen* aus. SnapManager zeigt das Dialogfeld Profilauthentifizierung an. 2. Geben Sie den Benutzernamen und das Kennwort des Hosts ein. SnapManager zeigt die Sicherungsliste an. Sie müssen das Profil nur einmal authentifizieren, solange die Anmeldeinformation en gültig sind und im Cache verbleiben.
Die GUI-Installation unter Windows ist erfolgreich, aber mit Fehlern.	Das Benutzerkonto, das zur Installation der GUI verwendet wird, verfügt nicht über ausreichende Berechtigungen, um die Symbole und Verknüpfungen für alle Benutzer einzurichten. Das Benutzerkonto verfügt nicht über die Berechtigung, das Verzeichnis C:\Dokumente und Einstellungen\Alle Benutzer zu ändern.	• Installieren Sie die GUI mit unterschiedlichen Einstellungen neu. Deaktivieren Sie unter Icon Verfügbarkeit auswählen das Kontrollkästchen **Diese Verknüpfungen allen Benutzern dieses PCs zur Verfügung stellen**. • Melden Sie sich mit einem Benutzerkonto an, das nicht eingeschränkt ist, und installieren Sie die GUI neu.

Wenn Sie das erste Repository in der GUI öffnen, wird eine Fehlermeldung wie die folgende angezeigt: Der Profilname XXXX wird mit dem zuvor geladenen Repository übereinander.	Identisch benannte Profile können nicht in einem Repository vorhanden sein. Sie können auch nur ein Repository gleichzeitig öffnen.	Verwenden Sie die widersprüchlichen Profile von zwei verschiedenen Betriebssystembenutzern oder benennen Sie das Profil um, indem Sie eine SQL-Anweisung für das Repository ausgeben: AKTUALISIEREN Sie SMO_33_PROFILE SET NAME = 'NEW_NAME' MIT DEM NAMEN = 'OLD_NAME'.
Eine Fehlermeldung ähnlich der folgenden wird angezeigt: SMO-01092: Repository kann nicht initialisiert werden repo1@ existiert nicht:repo1SMO-11006: Der Host kann nicht aufgelöst werden	Das Repository ist unzugänglich, vielleicht weil es nicht mehr existiert. Die GUI initialisiert die Liste der Repositorys aus der Anmeldedatei.	In der Fehlermeldung wird gefragt, ob Sie dieses Repository entfernen möchten, damit kein Versuch unternommen wird, es in der Zukunft zu laden. Wenn Sie nicht auf dieses Repository zugreifen müssen, klicken Sie auf **Löschen**, um es aus der GUI-Ansicht zu entfernen. Dadurch wird der Verweis auf das Repository in der Anmeldedatei entfernt, und die GUI versucht nicht, das Repository erneut zu laden.
SnapManager benötigt eine längere Zeit, um die Baumstruktur der Datenbank zu laden, und führt dazu, dass auf der SnapManager-Benutzeroberfläche eine Fehlermeldung mit einem Timeout angezeigt wird.	Wenn Sie versuchen, einen Teil-Backup-Vorgang von der SnapManager-Benutzeroberfläche auszuführen, versucht SnapManager, die Anmeldeinformationen für alle Profile zu laden. Wenn ungültige Einträge vorliegen, versucht SnapManager, den Eintrag zu validieren. Dies führt dazu, dass eine Fehlermeldung mit einem Timeout angezeigt wird.	Löschen Sie die Anmeldeinformationen des nicht verwendeten Hosts, Repositorys und Profils, indem Sie den Befehl zum Löschen von Anmeldeinformationen in der SnapManager-Befehlszeilenschnittstelle (CLI) verwenden.
Die benutzerdefinierten Skripte, die für die vor- oder Nachbearbeitungsaktivität vor oder nach dem Backup-, Restore- oder Klonvorgang ausgeführt werden, sind in der SnapManager GUI nicht sichtbar.	Wenn Sie nach dem Start des jeweiligen Assistenten benutzerdefinierte Skripts in den benutzerdefinierten Speicherort für Backup, Wiederherstellung oder Klonen hinzufügen, werden die benutzerdefinierten Skripts nicht unter der Liste Verfügbare Skripts angezeigt.	Starten Sie den SnapManager-Hostserver neu, und öffnen Sie dann die SnapManager-GUI.

Sie können die in SnapManager (3.1 oder früher) erstellte XML-Datei für die Klonspezifikation nicht verwenden.	Ab SnapManager 3.2 für Oracle wird der Abschnitt Aufgabenspezifikation (Task-Specification) als separate XML-Datei für die Aufgabenspezifikation bereitgestellt.	Wenn Sie SnapManager 3.2 für Oracle verwenden, müssen Sie den Abschnitt für die Aufgabenspezifikation aus der XML für die Klonspezifikation entfernen oder eine neue XML-Datei für die Klonspezifikation erstellen. SnapManager 3.3 oder höher unterstützt nicht die XML-Datei für die Klonspezifikation, die in SnapManager 3.2 oder älteren Versionen erstellt wurde.

Die SnapManager-Operation auf der Benutzeroberfläche wird nicht fortgesetzt, nachdem Sie die Benutzeranmeldeinformationen gelöscht haben, indem Sie den Befehl smo cumm clear von der SnapManager CLI verwenden oder durch Klicken auf **Admin** > **Anmeldeinformationen** > **Löschen** > **Cache** in der SnapManager-Benutzeroberfläche.	Die für Repositorys, Hosts und Profile festgelegten Anmeldeinformationen werden gelöscht. SnapManager überprüft vor dem Starten eines Vorgangs die Benutzeranmeldeinformationen.Wenn die Benutzeranmeldeinformationen ungültig sind, kann sich SnapManager nicht authentifizieren. Wenn ein Host oder ein Profil aus dem Repository gelöscht wird, sind die Benutzeranmeldeinformationen weiterhin im Cache verfügbar. Diese unnötigen Einträge mit Anmeldeinformationen verlangsamen die SnapManager-Vorgänge von der GUI.	Starten Sie die SnapManager GUI neu, je nachdem, wie der Cache gelöscht wird. **Hinweis:** • Wenn Sie den Anmeldeinformationscache von der SnapManager-GUI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche nicht beenden. • Wenn Sie den Anmeldeinformationscache über die SnapManager-CLI gelöscht haben, müssen Sie die SnapManager-Benutzeroberfläche neu starten. • Wenn Sie die verschlüsselte Anmeldedatei manuell gelöscht haben, müssen Sie die SnapManager-GUI neu starten. Legen Sie die Anmeldeinformationen fest, die Sie für das Repository, den Profilhost und das Profil angegeben haben. Wenn in der SnapManager-GUI kein Repository unter der Struktur Repositories zugeordnet ist, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf **Tasks** > **Exisiting Repository hinzufügen** 2. Klicken Sie mit der rechten Maustaste auf das Repository, klicken Sie auf **Öffnen** und geben Sie die Benutzeranmeldeinformationen im Fenster * Repository Credentials Authentication* ein. 3. Klicken Sie mit der rechten Maustaste auf den Host im Repository, klicken Sie auf **Öffnen** und geben Sie die Benutzeranmeldeinformationen in **Host Authentication** ein. 4. Klicken Sie mit der rechten Maustaste auf das Profil unter dem Host, klicken Sie auf **Öffnen** und geben Sie die Benutzeranmeldeinformationen in **Profilauthentifizierung** ein.

Sie können die SnapManager-Benutzeroberfläche nicht über die Java Web Start GUI öffnen, da die SSL-Verschlüsselung (Secure Sockets Layer) des Browsers schwächer ist.	SnapManager unterstützt keine SSL-Chiffren, die schwächer als 128 Bit sind.	Aktualisieren Sie die Browserversion und überprüfen Sie die Verschlüsselungsstärke.

Fehlerbehebung bei bekannten Problemen

Sie sollten einige bekannte Probleme kennen, die bei der Verwendung von SnapManager auftreten können, und deren Umgang damit.

SnapManager für Oracle erkennt Cluster-Mode-Profile nicht

Falls der Clustermodus-Profilname nicht in der Datei cmode_profiles.config im Installationsverzeichnis von SnapManager für Oracle vorhanden ist, kann die folgende Fehlermeldung auslösen:

Konfigurieren Sie bitte DFM Server mit SnapDrive config set -dfm user_Name Appliance_Name.

Wenn Sie auch bei der Aktualisierung der SnapManager für Oracle den Ordner /opt/NetApp/smo/* löschen, wird auch die Datei cmode_profil.config mit den Cluster-Mode-Profilnamen gelöscht. Dieses Problem löst auch die gleiche Fehlermeldung aus.

Workaround

Aktualisieren Sie das Profil: smo Profile Update-profile <profile_Name>

> Falls SnapManager für Oracle im Pfad /opt/NetApp/smo/ installiert ist, lautet der Dateispeicherort /opt/NetApp/smo/cmode_profile.config.

Der Server kann nicht gestartet werden

Beim Starten des Servers wird möglicherweise eine Fehlermeldung wie die folgende angezeigt:

SMO-01104: Fehler beim Aufrufen des Befehls: SMO-17107: Der SnapManager Server konnte aufgrund der folgenden Fehler nicht am Port 8074 gestartet werden: java.net.BindException: die Adresse wird bereits verwendet

Dies kann daran liegen, dass die SnapManager-Listening-Ports (standardmäßig 27214 und 27215) derzeit von einer anderen Anwendung verwendet werden.

Dieser Fehler kann auch auftreten, wenn der smo_Server-Befehl bereits ausgeführt wird, aber SnapManager erkennt den vorhandenen Prozess nicht.

Workaround

Sie können SnapManager oder die andere Anwendung neu konfigurieren, um unterschiedliche Ports zu verwenden.

Um SnapManager neu zu konfigurieren, bearbeiten Sie die folgende Datei: C:\Programme\NetApp\SnapManager für Oracle\Properties\smo.config

Sie weisen folgende Werte zu:

- SMO Server.Port = 27214
- SMO Server.rmiRegistry.Port=27215
- Remote.Registry.ocijdbc.Port= 27215

  Der Remote.Registry.ocijdbc.Port muss der gleiche sein wie der Server.rmiRegistry.Port.

So starten Sie den SnapManager-Server:

1. Klicken Sie Auf **Start** > **Systemsteuerung** > **Verwaltung** > **Services**.
2. Sie können den Server auf drei Arten starten:
   - Klicken Sie im linken Bereich auf **Start**.
   - Klicken Sie mit der rechten Maustaste auf NetApp SnapManager 3.3 für Oracle und wählen Sie im Dropdown-Menü die Option **Start** aus.
   - Doppelklicken Sie auf NetApp SnapManager 3.3 für Oracle und klicken Sie im Fenster Eigenschaften auf **Start**.

Zielnamen der Archivprotokolldatei können nicht verwaltet werden, wenn die Zielnamen Teil anderer Zielnamen sind

Wenn der Benutzer beim Erstellen einer Archiv-Log-Sicherung ein Ziel ausschließt, das Teil anderer Zielnamen ist, werden auch die anderen Zielnamen ausgeschlossen.

Nehmen wir beispielsweise an, dass drei Ziele ausgeschlossen werden können: E:\\Arch, G:\\Arch und H:\\Arch. Beim Erstellen der Backup der Archivprotokolldatei, wenn Sie E:\\ARCH mit dem Befehl ausschließen

```
smo backup create -profile almsamp1 -data -online -archivelogs  -exclude
-dest E:\\arch
```

, SnapManager für Oracle schließt alle Ziele ab, die mit E:\\ARCH beginnen.

Workaround

- Fügen Sie einen Pfadtrenner hinzu, nachdem Ziele in V€tarchiv_dest konfiguriert wurden. Ändern Sie z. B. den Bogen E:\\in E:\\Arch\.
- Bei der Erstellung eines Backups sollten Ziele berücksichtigt werden, anstatt Ziele auszuschließen.

Die Größe der Repository-Datenbank wächst mit der Zeit, nicht mit der Anzahl der Backups

Die Größe der Repository-Datenbank wächst mit der Zeit, da SnapManager-Operationen Daten innerhalb des Schemas in den Repository-Datenbanktabellen einfügen oder löschen, was zu einer hohen Indexbelegung führt.

Workaround

Sie müssen die Indizes gemäß den Oracle-Richtlinien überwachen und neu erstellen, um den vom Repository-Schema belegten Speicherplatz zu steuern.

Auf die SnapManager-Benutzeroberfläche kann nicht zugegriffen werden und SnapManager-Vorgänge schlagen fehl, wenn die Repository-Datenbank ausfällt

SnapManager-Vorgänge schlagen fehl und Sie können nicht auf die GUI zugreifen, wenn die Repository-Datenbank ausfällt.

In der folgenden Tabelle sind die verschiedenen Aktionen aufgeführt, die Sie ausführen möchten, sowie deren Ausnahmen:

Betrieb	Ausnahmen
Öffnen eines geschlossenen Repository	Die folgende Fehlermeldung wird in SM_gui.log: [WARNUNG]: SMO-01106: Beim Abfragen des Projektarchivs ist ein Fehler aufgetreten: Geschlossene Verbindung java.sql.SQLException: Geschlossene Verbindung.
Aktualisieren eines geöffneten Projektarchivs durch Drücken von F5	Eine Projektarchiv-Ausnahme wird in der GUI angezeigt und protokolliert auch eine NullPointerException in der Datei sm_gui.log.
Aktualisieren des Hostservers	Eine NullPointerException wird in der Datei sumo_gui.log protokolliert.
Erstellen eines neuen Profils	Im Fenster Profilkonfiguration wird eine NullPointerException angezeigt.
Aktualisieren eines Profils	Die folgende SQL-Ausnahme wird in SM_gui.log: [WARNUNG] protokolliert: SMO-01106: Beim Abfragen des Projektarchivs ist ein Fehler aufgetreten: Geschlossene Verbindung.
Zugriff auf ein Backup	Die folgende Fehlermeldung wird in SM_gui.log protokolliert: Die Initialisierung einer Sammlung konnte nicht abgeschlossen werden.
Anzeigen der Kloneigenschaften	Die folgende Fehlermeldung wird in sm_gui.log protokolliert und sumo_gui.log: Die Initialisierung einer Sammlung konnte nicht abgeschlossen werden.

Workaround

Sie müssen sicherstellen, dass die Repository-Datenbank ausgeführt wird, wenn Sie auf die GUI zugreifen möchten oder SnapManager-Vorgänge ausführen möchten.

Es können keine temporären Dateien für die geklonte Datenbank erstellt werden

Wenn temporäre Tablespaces-Dateien der Zieldatenbank in Mount-Punkten platziert werden, die sich vom Mount-Punkt der Datendateien unterscheiden, ist der Klonvorgang erfolgreich, SnapManager kann jedoch keine temporären Dateien für die geklonte Datenbank erstellen.

Workaround

Sie müssen einen der folgenden Schritte ausführen:

- Stellen Sie sicher, dass die Zieldatenbank so angelegt ist, dass temporäre Dateien an demselben Bereitstellungspunkt wie die der Datendateien abgelegt werden.
- Manuelles Erstellen oder Hinzufügen temporärer Dateien in der geklonten Datenbank.

Das Backup der Data Guard Standby-Datenbank ist fehlgeschlagen

Wenn ein Archivprotokoll mit dem Dienstnamen der primären Datenbank konfiguriert ist, schlägt die Datensicherung der Data Guard Standby-Datenbank fehl.

Workaround

In der GUI müssen Sie **External Archive Log Location** angeben, der dem Dienstnamen der primären Datenbank entspricht.

Ausführung mehrerer paralleler Vorgänge schlägt in SnapManager fehl

Wenn Sie mehrere parallele Vorgänge auf separaten Datenbanken ausführen, die sich im selben Storage-System befinden, wird die Initiatorgruppe für LUNs, die beiden Datenbanken zugeordnet sind, möglicherweise aufgrund eines der Vorgänge gelöscht. Wenn später der andere Vorgang versucht, die gelöschte Initiatorgruppe zu verwenden, zeigt SnapManager eine Fehlermeldung an.

Wenn beispielsweise Backup-Löschvorgänge und Backup-Erstellungsvorgänge für verschiedene Datenbanken nahezu gleichzeitig ausgeführt werden, schlägt der Backup-Vorgang fehl. Die folgenden sequenziellen Schritte zeigen, was passiert, wenn Sie Backup löschen und Backup erstellen Vorgänge auf verschiedenen Datenbanken fast gleichzeitig ausführen.

1. Führen Sie den Befehl Backup delete aus.
2. Führen Sie den Befehl Backup create aus.
3. Der Befehl zum Erstellen des Backups identifiziert die bereits vorhandene Initiatorgruppe und verwendet dieselbe Initiatorgruppe zum Zuordnen der LUN.
4. Der Befehl zum Löschen des Backups löscht die Backup-LUN, die derselben Initiatorgruppe zugeordnet war.
5. Mit dem Befehl „Backup löschen“ wird dann die Initiatorgruppe gelöscht, da der Initiatorgruppe keine LUNs zugeordnet sind.
6. Der Befehl „Backup create“ erstellt das Backup und versucht, der Initiatorgruppe, die nicht vorhanden ist, zuzuordnen. Somit schlägt der Vorgang fehl.

Was zu tun

Sie müssen eine Initiatorgruppe für jedes Storage-System erstellen, das von der Datenbank verwendet wird. Verwenden Sie dazu den folgenden Befehl: Sdcli igroup create

RAC-Datenbank kann von einem der RAC-Knoten, in dem das Profil nicht erstellt wurde, nicht wiederhergestellt werden

In einer Oracle RAC Umgebung, in der beide Nodes zum selben Cluster gehören, wenn Sie einen Wiederherstellungsvorgang von einem Node starten, der sich von dem Node,

an dem das Backup erstellt wurde, unterscheidet, schlägt der Wiederherstellungsvorgang fehl.

Wenn Sie beispielsweise in Knoten A ein Backup erstellen und versuchen, von Knoten B wiederherzustellen, schlägt der Wiederherstellungsvorgang fehl.

Was zu tun

Führen Sie vor dem Durchführen des Wiederherstellungsvorgangs von Node B folgende Schritte in Node B durch:

1. Fügen Sie das Repository hinzu.
2. Synchronisieren Sie das Profil, indem Sie das Kommando smo profile Sync ausführen.
3. Legen Sie die Anmeldeinformationen für das Profil fest, das für den Wiederherstellungsvorgang verwendet werden soll, indem Sie den Befehlssatz für Smo-Anmeldeinformationen ausführen.
4. Aktualisieren Sie das Profil, um den neuen Hostnamen und den entsprechenden SID hinzuzufügen, indem Sie den Befehl smo Profil aktualisieren.

Weitere Informationen

Hier finden Sie Informationen zu den grundlegenden Aufgaben, die bei der Installation und Verwendung von SnapManager anfallen.

Dokument An	Beschreibung
Beschreibungsseite „SnapManager“	Auf dieser Seite finden Sie Informationen über SnapManager, Verweise auf Online-Dokumentationen und einen Link zur SnapManager Download-Seite, von der aus Sie die Software herunterladen können.
Data ONTAP-SAN-Konfigurationsleitfaden für 7-Mode	Dieses Dokument ist unter verfügbar "mysupport.netapp.com". Es handelt sich um ein dynamisches Online-Dokument mit aktuellsten Informationen zu den Anforderungen für das Einrichten eines Systems in einer SAN-Umgebung. Er liefert die aktuellen Details zu Storage-Systemen und Host-Plattformen, Verkabelungsproblemen, Switch-Problemen und Konfigurationen.
Kompatibilitätsmatrix für SnapManager und SnapDrive	Dieses Dokument ist im Abschnitt Interoperabilität verfügbar unter "mysupport.netapp.com/matrix". Es handelt sich um ein dynamisches Online-Dokument, das die aktuellsten Informationen enthält, die für SnapManager und seine Plattformanforderungen spezifisch sind.

Versionshinweise zu SnapManager	Dieses Dokument ist mit SnapManager erhältlich. Sie können auch eine Kopie von herunterladen "mysupport.netapp.com". Es enthält alle Last-Minute-Informationen, damit die Konfiguration reibungslos ausgeführt werden kann.
Dokumentation von NetApp Host-Anschluss und Support-Kits	"mysupport.netapp.com".
Systemkonfigurationshandbuch	"mysupport.netapp.com".
Data ONTAP Block Access Management-Leitfaden	"mysupport.netapp.com"
Informationen zu Host-Betriebssystem und Datenbank	Diese Dokumente enthalten Informationen zu Ihrem Host-Betriebssystem und Ihrer Datenbanksoftware.

Klassifizierungen für Fehlermeldungen

Sie können die Ursache eines Fehlers bestimmen, wenn Sie die Klassifizierungen der Nachrichten kennen.

In der folgenden Tabelle finden Sie Informationen zu den numerischen Bereichen für die verschiedenen Meldungsarten, die Sie möglicherweise bei SnapManager sehen:

Gruppieren	Bereich	Zu Verwenden
UMGEBUNG	1000-1999	Wird verwendet, um den Zustand oder Probleme mit der Betriebsumgebung von SnapManager zu protokollieren. Diese Gruppe umfasst Meldungen über die Systeme, mit denen SnapManager interagiert, wie z. B. Host, Storage-System, Datenbank usw.
BACKUP	2000-2999	Verbunden mit dem Datenbank-Backup-Prozess.
WIEDERHERSTELLEN	3000-3999	Verknüpft mit dem Wiederherstellungsprozess der Datenbank.
KLON	4000-4999	Diesem Datenbankklonprozess zugeordnet.
PROFIL	5000-5999	Wird zum Verwalten von Profilen verwendet.

MANAGEN	6000-6999	Wird für das Management von Backups verwendet.
SCHNITTSTELLE FÜR VIRTUELLE DATENBANKEN	7000-7999	Der Schnittstelle der virtuellen Datenbank zugeordnet.
VIRTUAL STORAGE INTERFACE	8000-8999	Einer virtuellen Storage-Schnittstelle zugeordnet.
REPOSITORY	9000-9999	Der Repository-Schnittstelle zugeordnet.
METRIKEN	10000-10999	Zugeordnet zur Größe des Datenbank-Backups, verstrichene Zeit zum Backup, Zeit zur Wiederherstellung der Datenbank, die Anzahl der Male, die eine Datenbank geklont wurde usw.
VIRTUELLE HOST-SCHNITTSTELLE	11000-11999	Der virtuellen Host-Schnittstelle zugeordnet. Dies ist die Schnittstelle zum Host-Betriebssystem.
AUSFÜHRUNG	12000-12999	Verbunden mit dem Ausführungspaket, einschließlich Laichen und Verarbeitung von Betriebssystemaufrufen.
PROZESS	13000-13999	Verknüpft mit der Prozesskomponente von SnapManager.
VERSORGUNGSUNTERNEHMEN	14000-14999	Verbunden mit SnapManager Utilities, globalem Kontext usw.
DUMP/DIAGNOSE	15000-15999	Im Zusammenhang mit Dump- oder Diagnosevorgängen.
HILFE	16000-16999	Mit Hilfe verknüpft.
SERVER	17000-17999	Wird in der SnapManager-Serveradministration verwendet.
API	18000-18999	Der API zugeordnet.
AUTH	20000-20999	Mit der Autorisierung von Anmeldeinformationen verknüpft.

Fehlermeldungen

Sie finden Informationen zu den Fehlermeldungen, die mit verschiedenen SnapManager Vorgängen verbunden sind.

Die häufigsten Fehlermeldungen

Die folgende Tabelle enthält einige der häufigsten und wichtigsten Fehler im Zusammenhang mit SnapManager für Oracle:

Fehlermeldung	Erklärung	Auflösung
SD-10038: Dateisystem ist nicht beschreibbar.	Der SnapManager-Prozess hat keinen Schreibzugriff auf das Dateisystem.	Sie müssen sicherstellen, dass der SnapManager-Prozess Schreibzugriff auf das Dateisystem hat. Nach der Korrektur müssen Sie eventuell einen weiteren Snapshot erstellen.
SMO-05075: Profil konnte nicht erstellt werden. Sie müssen die DP/XDP-Beziehung entsprechend der zugrunde liegenden Beziehung richtig konfigurieren oder die richtige Schutzrichtlinie auswählen.	Die zugrunde liegenden Volumes befinden sich nicht in einer SnapVault oder SnapMirror Beziehung.	Sie müssen eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.
SMO-05503: Sie haben denselben Namen für das Profil angegeben. Geben Sie einen anderen Namen an, um das Profil umzubenennen.	Profile mit identischen Namen können nicht in einem Repository vorhanden sein.	Geben Sie einen Profilnamen an, der nicht verwendet wird.
SMO-05505: Die Metadaten des Datensatzes können nicht aktualisiert werden.	Datensatz wurde möglicherweise gelöscht oder ist nicht vorhanden.	Vergewissern Sie sich vor dem Aktualisieren der Datensatz-Metadaten, dass der Datensatz mithilfe der NetApp Management Console vorhanden ist.
SMO-05506: Sie können das Profil nicht aktualisieren, da auf dem Profil Operationen ausgeführt werden. Sie müssen warten, bis die Operation(en) abgeschlossen ist und dann das Profil aktualisieren.	Profil kann nicht aktualisiert werden, wenn Backup-, Wiederherstellungs- und Klonvorgänge ausgeführt werden.	Aktualisieren Sie das Profil nach Abschluss des aktuellen Vorgangs.
SMO-05509: Ungültige primäre Aufbewahrungsdauer beim Archivprotokoll - geben Sie einen positiven Ganzzahl an.	Die Aufbewahrungsdauer von Backups im Archivprotokoll kann nicht negativ sein.	Geben Sie einen positiven Wert für die Aufbewahrungsdauer von Archiv-Log-Backups an.

SMO-07463: Für diese Backup-Wiederherstellung muss die Datenbank im erforderlichen Zustand sein. Fehler beim Abrufen der Datenbank in den erforderlichen Zustand.	Die Datenbank befindet sich nicht im erforderlichen Zustand für einen Backup-Vorgang.	Überprüfen Sie, ob die Datenbank in einem relevanten Zustand ist, bevor Sie eine Backup-Kopie erstellen. Der Status der Datenbank, die wiederhergestellt werden soll, hängt von der Art des Wiederherstellungsprozesses, die Sie durchführen möchten, und der Art der Dateien ab, die enthalten sein sollen.
SMO-09315: Nach Durchführung von Repository-Upgrades oder -Updates erhalten Sie möglicherweise keine zusammenfassende Benachrichtigung für Benachrichtigungen, die in der vorherigen Version festgelegt wurden, es sei denn, Sie aktualisieren die Zusammenfassung Benachrichtigung mit den Details des Benachrichtigungs-Hosts.	Benachrichtigungseinstellungen sind nach einem Rolling Upgrade nicht für das Repository konfiguriert.	Aktualisieren Sie nach einem Rolling Upgrade die Benachrichtigungseinstellungen für die Zusammenfassung, um Benachrichtigungen zu erhalten.
SM0-02076: Der Name des Etiketts darf keine Sonderzeichen enthalten, die nicht unterstrich sind.	Der Name des Etiketts enthält Sonderzeichen, die nicht vom Unterstrich verwendet werden.	Der Name der Bezeichnung muss innerhalb des Profils eindeutig sein. Der Name kann Buchstaben, Zahlen, einen Unterstrich (_) und einen Bindestrich (-) enthalten (kann jedoch nicht mit einem Bindestrich beginnen). Achten Sie darauf, dass Etiketten keine Sonderzeichen enthalten, außer dem Unterstrich.
SMO-06308: Ausnahme beim Versuch, Zeitplan zu starten: java.lang.NullPointerException	Der vollständig qualifizierte Domänenname (FQDN) des Profilhosts ist anstelle des Host-Namens des Systems konfiguriert, und der FQDN des Profilhosts kann nicht aufgelöst werden.	Stellen Sie sicher, dass Sie den Hostnamen des Systems und nicht den FQDN verwenden.

Fehler in ExecuteRestoreSteps: ORACLE-10003: Fehler beim Ausführen von SQL "DROP DISKGROUP;Control diskgroup Name; INCL. INHALT" gegen Oracle-Datenbank +ASM1: ORA-15039: diskgroup not Drop ORA-15027: Aktive Nutzung der Diskgroup; "Control diskgroup Name;" schließt seine Dismount aus	Der Vorgang zum Wiederherstellen eines Backups mit Steuerdateien fällt nicht auf die Steuerplattengruppe. Dieses Problem tritt auf, wenn veraltete gesicherte Kontrolldateien in der Gruppe der Steuerdatenträger vorhanden sind.	Identifizieren Sie die veralteten gesicherten Kontrolldateien, und löschen Sie sie manuell.
RMAN-06004: ORACLE-Fehler aus der Datenbank des Wiederherstellungskatalogs: ORA-01424: Fehlende oder unzulässige Zeichen nach dem Escape-Zeichen	Beim Erstellen des Backups konnte die Backup-Kopie nicht aus dem Katalog entfernt werden, wenn SnapManager in RMAN integriert ist.	Überprüfen Sie, ob externe Skripts zum Entfernen der Backups aus RMAN verwendet werden. Führen Sie DEN CROSSCHECK-BACKUP-Befehl in RMAN aus, um das RMAN-Repository zu aktualisieren und den Befehl „Resynchronisieren“-Katalog, um die Steuerdatei der Zieldatenbank mit dem Wiederherstellungskatalog zu synchronisieren.
[DEBUG]: Ausnahme beim Beschneiden von Backups. java.lang.IllegalStelleException: [Assertion failed] - dieser Zustand invariant muss wahr sein	Mehrere Snapshot Kopien werden für eine einzige Operation ID erstellt.	Löschen Sie die Snapshot-Kopien manuell, und löschen Sie die Einträge mithilfe von Skripten aus dem Repository.
Die Systemzeit und die von SnapManager in den Protokolldateien angezeigte Zeit stimmen nicht überein oder nicht synchronisiert.	Eine Änderung der Zeitzone wird von Java 7 noch nicht unterstützt.	Wenden Sie den von Oracle bereitgestellten tzupdater-Patch an.
DISC-00001: Speicher kann nicht gefunden werden: Die folgende Kennung existiert nicht oder ist nicht vom erwarteten Typ: ASM-Datei	Daten- oder Kontrolldateien oder Redo-Logs werden in einer ASM-Datenbank multipliziert.	Entfernen Sie das Oracle Multiplexing.

ORA-01031: Unzureichende Berechtigungen. Überprüfen Sie, ob der SnapManager-Windows-Dienst so eingerichtet ist, dass er als Benutzer mit den richtigen Berechtigungen ausgeführt wird und dass der Benutzer in die ORA_DBA-Gruppe aufgenommen wurde.	In SnapManager verfügen Sie über unzureichende Berechtigungen. Das SnapManager-Dienstkonto ist nicht Teil der ORA_DBA-Gruppe.	Klicken Sie mit der rechten Maustaste auf das Symbol **Computer** auf Ihrem Desktop und wählen Sie **Verwalten** aus, um zu überprüfen, ob das Benutzerkonto für den SnapManager-Dienst Teil der ORA_DBA-Gruppe ist. Überprüfen Sie lokale Benutzer und Gruppen und stellen Sie sicher, dass das Konto Teil der ORA_DBA-Gruppe ist. Wenn der Benutzer der lokale Administrator ist, stellen Sie sicher, dass sich der Benutzer in der Gruppe und nicht in der Domain-Administrator befindet.
0001-SMO-02016: Es können externe Tabellen in der Datenbank vorhanden sein, die nicht im Rahmen dieses Backup gesichert wurden (da die Datenbank während dieses Backups nicht GEÖFFNET war, konnten ALL_EXTERNAL_LOCATIONS nicht abgefragt werden, um festzustellen, ob externe Tabellen vorhanden sind oder nicht).	Externe Tabellen werden von SnapManager nicht gesichert (z. B. Tabellen, die nicht in .dbf-Dateien gespeichert sind). Dieses Problem tritt auf, weil die Datenbank während des Backups nicht geöffnet war. SnapManager kann nicht bestimmen, ob externe Tabellen verwendet werden.	Möglicherweise gab es externe Tabellen in der Datenbank, die im Rahmen dieses Vorgangs nicht gesichert wurden (da die Datenbank während des Backups nicht geöffnet war).
0002-332 Admin-Fehler: SD.Snapshot.Clone-Zugriff auf Volume „Volume_Name“ für Benutzer-Benutzername auf Operations Manager Server(s) „dfm_Server“ konnte nicht überprüft werden. Grund: Ungültige Ressource angegeben. Kann seine ID auf Operations Manager Server „dfm_Server“ nicht finden	Die richtigen Zugriffsberechtigungen und Rollen sind nicht festgelegt.	Legen Sie Zugriffsberechtigungen oder -Rollen für die Benutzer fest, die versuchen, den Befehl auszuführen.
[WARNUNG] FLOW-11011: Vorgang abgebrochen [FEHLER] FLOW-11008: Vorgang fehlgeschlagen: Java-Heap-Speicherplatz.	Die Datenbank enthält mehr Archivprotokolldateien als die maximal zulässige Anzahl.	1. Navigieren Sie zum Installationsverzeichnis für SnapManager. 2. Öffnen Sie die Datei Launch-java. 3. Erhöhen Sie den Wert des `java -Xmx160m` Java Heap Space Parameter . So können Sie beispielsweise den Wert vom Standardwert von 160m bis 200m AS ändern `java -Xmx200m`.

SMO-21019: Fehler beim Beschneiden des Archivprotokolls für das Ziel: "E:\dest" mit dem Grund: "ORACLE-00101: Fehler beim Ausführen des RMAN-Befehls: [LÖSCHEN NOPROMPT ARCHIVELOG 'E:\dest']"	Die Beschneidung des Archivprotokolls schlägt in einem der Ziele fehl. In einem solchen Szenario, SnapManager weiterhin die Archiv-Log-Dateien aus den anderen Zielen zu beschneiden. Wenn Dateien manuell aus dem aktiven Dateisystem gelöscht werden, kann RMAN die Archivprotokolldateien nicht von diesem Ziel beschneiden.	Verbinden Sie sich über den SnapManager-Host mit RMAN. Führen Sie den Befehl RMAN CROSSCHECK ARCHIVELOG ALL aus und führen Sie den Beschneiungsvorgang für die Archivprotokolldateien erneut durch.
SMO-13032: Vorgang kann nicht ausgeführt werden: Archiv-Log Prune. Root Cause: RMAN Ausnahme: ORACLE-00101: Fehler beim Ausführen des RMAN Befehls.	Die Archivprotokolldateien werden manuell aus den Speicherprotokollzielen gelöscht.	Verbinden Sie sich über den SnapManager-Host mit RMAN. Führen Sie den Befehl RMAN CROSSCHECK ARCHIVELOG ALL aus und führen Sie den Beschneiungsvorgang für die Archivprotokolldateien erneut durch.
Shell-Ausgabe konnte nicht analysiert werden: (java.util.regex.Matcher[pattern=Befehl abgeschlossen. Region=0,18 lastmatch=]) stimmt nicht überein (Name:Backup_script) Shell-Ausgabe konnte nicht analysiert werden (java.util.regex.Matcher[pattern=Befehl abgeschlossen. Region=0,25 lastmatch=]) stimmt nicht überein (Beschreibung:Sicherungsskript) Shell-Ausgabe konnte nicht analysiert werden: (java.util.regex.Matcher[pattern=Befehl abgeschlossen. Region=0,9 lastmatch=]) stimmt nicht überein (Timeout:0)	Umgebungsvariablen werden in den Skripten vor oder nach der Aufgabe nicht richtig festgelegt.	Überprüfen Sie, ob die vor- oder Nachaufgaben-Skripte der Standard-SnapManager-Plug-in-Struktur entsprechen. Weitere Informationen über die Verwendung der Umgebungsvariablen im Skript finden Sie unter Vorgänge in Taskskripten.

ORA-01450: Maximale Schlüssellänge (6398) überschritten.	Wenn Sie ein Upgrade von SnapManager 3.2 für Oracle auf SnapManager 3.3 für Oracle durchführen, schlägt der Aktualisierungsvorgang mit dieser Fehlermeldung fehl. Dieses Problem kann aus einem der folgenden Gründe auftreten: • Die Blockgröße des Tablespaces, in dem das Repository vorhanden ist, beträgt weniger als 8 KB. • der parameter nls_length_semantik wird auf char gesetzt.	Sie müssen die Werte den folgenden Parametern zuweisen: • Block_size=8192 • nls_length=Byte Nach dem Ändern der Parameterwerte müssen Sie die Datenbank neu starten. Weitere Informationen finden Sie im Knowledge Base-Artikel 2017632.

Fehlermeldungen im Zusammenhang mit dem Datenbank-Backup-Prozess (Serie 2000)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die bei der Datensicherung der Datenbank auftreten:

Fehlermeldung	Erklärung	Auflösung
SMO-02066: Sie können die Archiv-Log-Sicherung „Data-logs“ nicht löschen oder freigeben, da der Backup mit Daten-Backup „Data-logs“ verknüpft ist.	Die Sicherung des Archivprotokolls wird zusammen mit der Datensicherung der Datendateien erstellt, und Sie haben versucht, die Sicherung des Archivprotokolls zu löschen.	Verwenden Sie die Option -Force, um die Sicherung zu löschen oder zu löschen.
SMO-02067: Sie können das Archivprotokoll-Backup „Data-Logs“ nicht löschen oder freigeben, da der Backup mit der Daten-Backup „Data-Logs“ verknüpft ist und innerhalb der zugewiesenen Aufbewahrungsdauer liegt.	Die Sicherung des Archivprotokolls ist mit dem Datenbank-Backup verknüpft und befindet sich innerhalb des Aufbewahrungszeitraums, und Sie haben versucht, das Backup des Archivprotokolls zu löschen.	Verwenden Sie die Option -Force, um die Sicherung zu löschen oder zu löschen.
SMO-07142: Archivierte Protokolle werden aufgrund des Ausschlussmusters <Ausschlussmuster> Pattern ausgeschlossen.	Während der Erstellung von Profilen oder Sicherungskopien werden einige Archivprotokolldateien ausgeschlossen.	Es ist keine Aktion erforderlich.

SMO-07155: <count> archivierte Log-Dateien sind nicht im aktiven File System vorhanden. Diese archivierten Protokolldateien werden nicht in die Sicherung aufgenommen.	Die Archivprotokolldateien sind während der Erstellung von Profilen oder Backups nicht im aktiven Dateisystem vorhanden. Diese archivierten Log-Dateien sind nicht im Backup enthalten.	Es ist keine Aktion erforderlich.
SMO-07148: Archivierte Log-Dateien sind nicht verfügbar.	Während der Profilerstellung oder der Sicherungserstellung werden für die aktuelle Datenbank keine Archivprotokolldateien erstellt.	Es ist keine Aktion erforderlich.
SMO-07150: Archivierte Log-Dateien wurden nicht gefunden.	Alle Archivprotokolldateien fehlen im Dateisystem oder werden während der Erstellung von Profilen oder Backups ausgeschlossen.	Es ist keine Aktion erforderlich.
SMO-13032: Backup Create kann nicht durchgeführt werden. Ursache: ORACLE-20001: Fehler beim Versuch, Status zu ändern, um FÜR Datenbank-Instanz ZU ÖFFNEN dfcln1: ORACLE-20004: Es wird erwartet, die Datenbank ohne die RESETLOGS-Option zu öffnen, aber oracle berichtet, dass die Datenbank mit der RESETLOGS-Option geöffnet werden muss. Um das unerwartete Zurücksetzen der Protokolle zu verhindern, wird der Prozess nicht fortgesetzt. Bitte stellen Sie sicher, dass die Datenbank ohne die RESETLOGS-Option geöffnet werden kann, und versuchen Sie es erneut.	Sie versuchen, die geklonte Datenbank zu sichern, die mit der Option -no-resetlogs erstellt wurde. Die geklonte Datenbank ist keine vollständige Datenbank.Sie können jedoch SnapManager Vorgänge wie das Erstellen von Profilen und Backups usw. mit der geklonten Datenbank ausführen, SnapManager die Vorgänge jedoch fehlschlagen, weil die geklonte Datenbank nicht als vollständige Datenbank konfiguriert ist.	Stellen Sie die geklonte Datenbank wieder her, oder konvertieren Sie die Datenbank in eine Data Guard Standby Datenbank.

Fehlermeldungen im Zusammenhang mit dem Wiederherstellungsprozess (Serie 3000)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die bei der Wiederherstellung auftreten:

Fehlermeldung	Erklärung	Auflösung

SMO-03031:Restore-Spezifikation ist zur Wiederherstellung von Backup <variabel> erforderlich, da die Storage-Ressourcen für das Backup bereits freigegeben wurden.	Sie haben versucht, ein Backup wiederherzustellen, bei dem die Speicherressourcen freigegeben werden, ohne eine Wiederherstellungsspezifikation anzugeben.	Geben Sie eine Wiederherstellungsspezifikation an.
SMO-03032:Restore-Spezifikation muss Zuordnungen für die wiederherzustellenden Dateien enthalten, da die Speicherressourcen für das Backup bereits freigegeben wurden. Die Dateien, für die Zuordnungen erforderlich sind, sind: <variabel> aus Snapshots: <Variable>	Sie haben versucht, ein Backup wiederherzustellen, bei dem die Speicherressourcen entlastet wurden, und eine Wiederherstellungsspezifikation, die keine Zuordnung für alle wiederherzustellenden Dateien enthält.	Korrigieren Sie die Spezifikationsdatei für die Wiederherstellung, damit die Zuordnungen mit den wiederherzustellenden Dateien übereinstimmen.

ORACLE-30028: Protokolldatei <Dateiname> kann nicht gespeichert werden. Die Datei ist möglicherweise nicht verfügbar/nicht zugänglich/beschädigt. Diese Protokolldatei wird nicht für die Wiederherstellung verwendet.	Die Online-Redo-Log-Dateien oder Archivprotokolldateien können nicht für die Wiederherstellung verwendet werden.dieser Fehler tritt aus folgenden Gründen auf: • Die in der Fehlermeldung erwähnten Online-Redo-Log-Dateien oder archivierten Log-Dateien verfügen nicht über ausreichende Änderungsnummern, um sie für die Wiederherstellung zu beantragen. Dies geschieht, wenn die Datenbank ohne Transaktionen online ist. Das Wiederherstellungsprotokoll oder die archivierten Protokolldateien verfügen über keine gültigen Änderungsnummern, die für die Wiederherstellung angewendet werden können. • Die in der Fehlermeldung erwähnte Online-Redo-Log-Datei oder archivierte Log-Datei verfügt nicht über ausreichende Zugriffsberechtigungen für Oracle. • Die in der Fehlermeldung erwähnte Online-Redo-Log-Datei oder archivierte Log-Datei ist beschädigt und kann nicht von Oracle gelesen werden. • Die in der Fehlermeldung erwähnte Online-Protokolldatei für Wiederherstellungen oder archivierte Log-Datei wurde in dem angegebenen Pfad nicht gefunden.	Wenn es sich bei der in der Fehlermeldung genannten Datei um eine archivierte Protokolldatei handelt und wenn Sie manuell für die Wiederherstellung angegeben haben, stellen Sie sicher, dass die Datei über alle Zugriffsrechte für Oracle verfügt.selbst wenn die Datei über volle Berechtigungen verfügt, Und die Meldung wird fortgesetzt, die Archivprotokolldatei enthält keine Änderungsnummern, die für die Wiederherstellung angewendet werden müssen, und diese Meldung kann ignoriert werden.

Fehlermeldungen, die mit dem Klonprozess verbunden sind (4000 Serie)

In der folgenden Tabelle sind die Fehler aufgeführt, die bei dem Klonprozess auftreten:

Fehlermeldung	Erklärung	Auflösung

SMO-04133: Dump-Ziel darf nicht vorhanden sein	Sie verwenden SnapManager zum Erstellen neuer Klone, jedoch sind die Dump-Ziele, die vom neuen Klon verwendet werden sollen, bereits vorhanden. SnapManager kann keinen Klon erstellen, wenn die Dump-Ziele vorhanden sind.	Entfernen oder umbenennen der alten Dump-Ziele, bevor Sie einen Klon erstellen.
SMO-13032:Vorgang kann nicht ausgeführt werden: Clone Create. Ursache: ORACLE-00001: Fehler beim Ausführen von SQL: [DATENBANK ÄNDERN ÖFFNEN RESETLOGS;]. Der zurückgegebene Befehl: ORA-38856: Kann Instanz NICHT als UNNAMED_INSTANCE_2 (Redo Thread 2) als aktiviert markieren.	Die Klonerstellung schlägt fehl, wenn Sie den Klon mit dem folgenden Setup aus der Standby-Datenbank erstellen: • Der Standby-Modus wird mithilfe von RMAN für das Backup der Datendateien erstellt.	Fügen Sie vor dem Erstellen des Klons den Parameter _no_Recovery_through_resetlogs= TRUE in die Klon-Spezifikations-Datei hinzu. Weitere Informationen finden Sie in der Oracle-Dokumentation (ID 334899.1). Stellen Sie sicher, dass Sie Ihren Oracle metalink-Benutzernamen und Ihr Kennwort haben.
	Sie haben in der Klon-Spezifikations-Datei keinen Wert für einen Parameter angegeben.	Sie müssen entweder einen Wert für den Parameter angeben oder diesen Parameter löschen, wenn er in der Klon-Spezifikations-Datei nicht erforderlich ist.

Fehlermeldungen im Zusammenhang mit der Verwaltung des Profilprozesses (5000-Serie)

In der folgenden Tabelle sind die Fehler aufgeführt, die bei dem Klonprozess auftreten:

Fehlermeldung	Erklärung	Auflösung
SMO-20600: Profil „profil1“ nicht im Repository "repo_Name" gefunden. Aktualisieren Sie bitte Ihre Profil-zu-Repository-Zuordnungen mit „Profile Sync“.	Der Dump-Vorgang kann nicht ausgeführt werden, wenn die Profilerstellung fehlschlägt.	Verwenden Sie den Smosystem-Dump.

Fehlermeldungen im Zusammenhang mit der Entlastung von Backup-Ressourcen (Backups 6000 Serie)

Die folgende Tabelle zeigt die häufigsten Fehler bei Backup-Aufgaben:

Fehlermeldung	Erklärung	Auflösung

SMO-06030: Backup kann nicht entfernt werden, da er in Verwendung ist: <Variable>	Sie haben versucht, den freien Vorgang für Backups mithilfe von Befehlen durchzuführen, wenn das Backup gemountet oder über Klone verfügt oder als unbegrenzt aufbewahrt werden soll.	Heben Sie die Bereitstellung des Backups auf, oder ändern Sie die Richtlinie für unbegrenzte Aufbewahrung. Sind Klone vorhanden, löschen Sie diese.
SMO-06045: Kann Backups nicht kostenlos erstellen <variabel>, da die Speicherressourcen für das Backup bereits freigegeben wurden	Sie haben versucht, den freien Vorgang des Backups über Befehle auszuführen, wenn das Backup bereits freigegeben wurde.	Sie können das Backup nicht freigeben, wenn es bereits freigegeben ist.
SMO-06047: Es können nur erfolgreiche Backups freigegeben werden. Der Status des Backups <ID> lautet <Status>.	Sie haben versucht, den kostenlosen Backup-Vorgang mithilfe von Befehlen auszuführen, wenn der Backup-Status nicht erfolgreich war.	Versuchen Sie es nach einer erfolgreichen Sicherung erneut.
SMO-13082: Vorgang kann nicht <variabel> für Backup <ID> ausgeführt werden, da die Storage-Ressourcen für das Backup freigegeben wurden.	Mit Befehlen haben Sie versucht, ein Backup bereitzustellen, das die Speicherressourcen freigegeben hat.	Sie können ein Backup, das die entsprechenden Storage-Ressourcen freigegeben hat, nicht mounten, klonen oder überprüfen.

Fehlermeldungen zum Rolling Upgrade-Prozess (Serie 9000)

In der folgenden Tabelle sind die häufigsten Fehler beim Rolling Upgrade aufgeführt:

Fehlermeldung	Erklärung	Auflösung
SMO-09234:die folgenden Hosts sind nicht im alten Repository vorhanden. <Hostnamen>	Sie haben versucht, ein Rolling Upgrade eines Hosts durchzuführen, der in der vorherigen Repository-Version nicht vorhanden ist.	Überprüfen Sie, ob der Host im vorherigen Repository vorhanden ist, indem Sie den Befehl Repository show-Repository aus der früheren Version der SnapManager-CLI verwenden.
SMO-09255:die folgenden Hosts sind nicht im neuen Repository vorhanden. <Hostnamen>	Sie haben versucht, ein Rollback eines Hosts durchzuführen, der in der neuen Repository-Version nicht vorhanden ist.	Überprüfen Sie, ob der Host im neuen Repository mit dem Befehl Repository show-Repository von der späteren Version der SnapManager-CLI vorhanden ist.
SMO-09256:Rollback wird nicht unterstützt, da neue Profile <Profilnamen>.für die angegebenen Hosts <Hostnamen> vorhanden sind.	Sie haben versucht, einen Host mit neuen im Repository vorhandenen Profilen wiederherzustellen. Diese Profile waren jedoch im Host der früheren SnapManager-Version nicht vorhanden.	Neue Profile in der neueren oder aktualisierten Version von SnapManager vor dem Rollback löschen.

SMO-09257:Rollback wird nicht unterstützt, da die Backups <Backupid> auf den neuen Hosts installiert sind.	Sie haben versucht, eine neuere Version des SnapManager-Hosts, der Backups gemountet hat, wiederherzustellen. Diese Backups werden in der früheren Version des SnapManager Hosts nicht eingebunden.	Heben Sie die Bereitstellung der Backups in der neueren Version des SnapManager Hosts auf, und führen Sie dann das Rollback durch.
SMO-09258:Rollback wird nicht unterstützt, da die Backups <Backupid> auf den neuen Hosts abgehängt werden.	Sie haben versucht, eine neuere Version des SnapManager-Hosts mit Backups, die nicht abgehängt werden, wiederherzustellen.	Mounten Sie die Backups in der neueren Version des SnapManager Hosts und führen Sie dann das Rollback durch.
SMO-09298:Dieses Repository kann nicht aktualisiert werden, da es bereits andere Hosts in der höheren Version hat. Führen Sie stattdessen ein RollingUpgrade für alle Hosts durch.	Sie haben ein Rolling Upgrade auf einem einzelnen Host durchgeführt und dann das Repository für diesen Host aktualisiert.	Führen Sie ein Rolling Upgrade auf allen Hosts durch.
SMO-09297: Fehler beim Aktivieren der Einschränkungen. Das Repository ist möglicherweise inkonsistent. Es wird empfohlen, das Backup des Repository, das Sie vor dem aktuellen Vorgang erstellt haben, wiederherzustellen.	Sie haben versucht, ein Rolling Upgrade oder einen Rollback-Vorgang durchzuführen, wenn die Repository-Datenbank in einem inkonsistenten Zustand bleibt.	Stellen Sie das zuvor gesicherte Repository wieder her.

Ausführung von Operationen (12,000 Serie)

In der folgenden Tabelle sind die häufigsten Fehler bei den Vorgängen aufgeführt:

Fehlermeldung	Erklärung	Auflösung
SMO-12347 [FEHLER]: SnapManager-Server wird nicht auf Host <Host> und Port <Port> ausgeführt. Führen Sie diesen Befehl auf einem Host aus, auf dem der SnapManager-Server ausgeführt wird.	Beim Einrichten des Profils haben Sie Informationen über den Host und Port eingegeben. SnapManager kann diese Vorgänge jedoch nicht ausführen, da der SnapManager-Server nicht auf dem angegebenen Host und Port ausgeführt wird.	Geben Sie den Befehl auf einem Host ein, auf dem der SnapManager-Server ausgeführt wird. Sie können den Port mit dem Befehl lsnrctl Status überprüfen und den Port anzeigen, auf dem die Datenbank ausgeführt wird. Ändern Sie bei Bedarf den Port im Backup-Befehl.

Ausführung von Prozesskomponenten (Serie 13,000)

In der folgenden Tabelle sind die häufigsten Fehler aufgeführt, die mit der Prozesskomponente von SnapManager verbunden sind:

Fehlermeldung	Erklärung	Auflösung

SMO-13083: Snapname-Muster mit dem Wert „x“ enthält Zeichen außer Buchstaben, Zahlen, Unterstrich, Bindestrich und geschweifte Klammern.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst. Sie haben jedoch Sonderzeichen enthalten, die nicht zulässig sind.	Entfernen Sie Sonderzeichen mit Ausnahme von Buchstaben, Zahlen, Unterstrichen, Bindestrich und geschweiften Klammern.
SMO-13084: Das Snapname-Muster mit dem Wert „x“ enthält nicht die gleiche Anzahl von linken und rechten Klammern.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst. Die linke und rechte geschweifte Klammern stimmen jedoch nicht überein.	Geben Sie im Snapname-Muster passende Öffnungs- und schließende Klammern ein.
SMO-13085: Das Snapname-Muster mit dem Wert „x“ enthält einen ungültigen Variablennamen von „y“.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst. Sie haben jedoch eine Variable enthalten, die nicht zulässig ist.	Entfernen Sie die beleidende Variable. Eine Liste der zulässigen Variablen finden Sie unter Benennen von Snapshot-Kopien.
SMO-13086 Snapname-Muster mit dem Wert „x“ muss die Variable „smid“ enthalten.	Beim Erstellen eines Profils haben Sie das Snapname-Muster angepasst; Sie haben jedoch die erforderliche smid-Variable weggelassen.	Geben Sie die erforderliche smid-Variable ein.

Fehlermeldungen zu SnapManager Utilities (14,000 Series)

Die folgende Tabelle zeigt die häufigsten Fehler im Zusammenhang mit SnapManager-Dienstprogrammen:

Fehlermeldung	Erklärung	Auflösung
SMO-14501: E-Mail-ID darf nicht leer sein.	Sie haben die E-Mail-Adresse nicht eingegeben.	Geben Sie eine gültige E-Mail-Adresse ein.
SMO-14502: E-Mail-Betreff darf nicht leer sein.	Sie haben den Betreff der E-Mail nicht eingegeben.	Geben Sie den entsprechenden E-Mail-Betreff ein.
SMO-14506: Das Feld für den E-Mail-Server darf nicht leer sein.	Sie haben den Hostnamen oder die IP-Adresse des E-Mail-Servers nicht eingegeben.	Geben Sie den gültigen Hostnamen oder die IP-Adresse des Mail-Servers ein.
SMO-14507: Das Feld „Mail-Port“ darf nicht leer sein.	Sie haben die E-Mail-Portnummer nicht eingegeben.	Geben Sie die Anschlussnummer des E-Mail-Servers ein.
SMO-14508: From Mail ID darf nicht leer sein.	Sie haben die E-Mail-Adresse des Absenders nicht eingegeben.	Geben Sie die E-Mail-Adresse eines gültigen Absenders ein.
SMO-14509: Benutzername darf nicht leer sein.	Sie haben die Authentifizierung aktiviert und den Benutzernamen nicht angegeben.	Geben Sie den Benutzernamen für die E-Mail-Authentifizierung ein.

SMO-14510: Das Passwort darf nicht leer sein. Geben Sie das Passwort ein.	Sie haben die Authentifizierung aktiviert und kein Passwort angegeben.	Geben Sie das E-Mail-Authentifizierungskennwort ein.
SMO-14550: E-Mail-Status <Erfolg/Ausfall>	Die Port-Nummer, der Mail-Server oder die E-Mail-Adresse des Empfängers sind ungültig.	Geben Sie bei der E-Mail-Konfiguration korrekte Werte an.
SMO-14559: Senden der E-Mail-Benachrichtigung fehlgeschlagen: <error>.	Dies kann auf eine ungültige Portnummer, einen ungültigen Mailserver oder eine ungültige E-Mail-Adresse des Empfängers zurückzuführen sein.	Geben Sie bei der E-Mail-Konfiguration korrekte Werte an.
SMO-14560: Benachrichtigung fehlgeschlagen: Die Benachrichtigungskonfiguration ist nicht verfügbar.	Senden der Benachrichtigung fehlgeschlagen, da die Benachrichtigungskonfiguration nicht verfügbar ist.	Benachrichtigungskonfiguration hinzufügen
SMO-14565: Ungültiges Zeitformat. Geben Sie das Zeitformat in HH:mm ein.	Sie haben die Uhrzeit in einem falschen Format eingegeben.	Geben Sie die Uhrzeit im Format hh:mm ein.
SMO-14566: Ungültiger Datumswert. Gültiger Datumsbereich: 1-31.	Das konfigurierte Datum ist falsch.	Das Datum muss zwischen 1 und 31 liegen.
SMO-14567: Ungültiger Tagewert. Gültiger Tagesbereich: 1-7.	Der konfigurierte Tag ist falsch.	Geben Sie den Tagesbereich zwischen 1 und 7 ein.
SMO-14569: Der Server konnte den Terminplan für die Zusammenfassung nicht starten.	Der SnapManager-Server wurde aus unbekannten Gründen heruntergefahren.	Starten Sie den SnapManager-Server.
SMO-14570: Benachrichtigung über Zusammenfassung nicht verfügbar.	Sie haben keine Übersichtsbenachrichtigung konfiguriert.	Konfigurieren Sie die zusammenfassende Benachrichtigung.
SMO-14571: Profil- und zusammenfassende Benachrichtigungen können nicht aktiviert werden.	Sie haben die Benachrichtigungsoptionen für Profil und Zusammenfassung ausgewählt.	Aktivieren Sie die Profilbenachrichtigung oder die Übersichtbenachrichtigung.
SMO-14572: Bieten Sie Erfolg- oder Fehleroption zur Benachrichtigung.	Sie haben die Erfolgs- oder Fehleroptionen nicht aktiviert.	Sie müssen entweder die Option Erfolg oder Fehler oder beides auswählen.

Verwandte Informationen

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 zu SnapManager für Oracle"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.